Fall 2022, Math 522: Week 15 Problem Set
Due: Monday, December 12th, 2022
Cyclotomic Polynomials

Discussion problems. The problems below should be worked on in class.

(D1) *Finding cyclotomic polynomials.* Factor $x^n - 1$ as a product of cyclotomic polynomials for each of the following values of n. Identify each factor as $\Phi_d(x)$ for some $d \mid n$.

Hint: you may find the following formulas useful.

$$a^2 - 1 = (a+1)(a-1), \qquad a^3 - 1 = (a-1)(a^2+a+1), \qquad a^3 + 1 = (a+1)(a^2-a+1)$$

(a) $n = 3$, $n = 9$, and $n = 16$.
(b) $n = 18$ (hint: $\Phi_{18}(x)$ has 3 nonzero terms)
(c) $n = 24$ (hint: $\Phi_{24}(x)$ has 3 nonzero terms)

(D2) *Some general formulas.*

(a) Find $\Phi_p(x)$ for p prime.
(b) Find $\Phi_n(x)$ when $n = 2^k$ for some $k \geq 1$. Prove your formula holds.
Hint: use induction on k.
(c) Compute $\Phi_n(-1)$ for each odd $n \leq 10$.
(d) Conjecture and prove a general formula for $\Phi_n(-1)$ when $n > 1$ is odd.
(e) Find $\Phi_n(x)$ when $n = 3^k$ for some $k \geq 1$. Prove your formula holds.

(D3) *Dirichlet's Theorem.* The goal of this problem is to use cyclotomic polynomials to prove the following special case of Dirichlet's theorem.

Theorem. *For each $n \geq 2$, there exist infinitely many primes equivalent to 1 modulo n.*

(a) Let $f(x) = \Phi_1(x)\Phi_2(x)\cdots\Phi_{n-1}(x)$. Argue that $f(x)$ and $\Phi_n(x)$ are coprime in $\mathbb{Q}[x]$.
Hint: consider the roots of $f(x)$ and $\Phi_n(x)$.
(b) Conclude $a(x)f(x) + b(x)\Phi_n(x) = 1$ for some $a(x), b(x) \in \mathbb{Q}[x]$.
(c) Conclude $A(x)f(x) + B(x)\Phi_n(x) = N$ for some $N \in \mathbb{Z}_{\geq 1}$ and $A(x), B(x) \in \mathbb{Z}[x]$.
(d) Fill in the blanks in the proof of the following lemma.

Lemma. *If $p > N$ is prime and $p \mid \Phi_n(b)$ for some $b \in \mathbb{Z}$, then $p \equiv 1 \bmod n$.*

Proof. Suppose $p \mid \Phi_n(b)$ for some $b \in \mathbb{Z}$. Since $\Phi_n(x) \mid$ _______, we must have $p \mid (b^n - 1)$, and thus $b^n \equiv 1 \bmod p$. We claim b has multiplicative order n modulo p. Indeed, if $b^k \equiv 1 \bmod p$ for some $k < n$, then $p \mid \Phi_d(b)$ for some $d \mid$ ____, meaning

$$A(b)f(b) + B(b)\Phi_n(b) = \_\_\_\_$$

is a multiple of p, which is impossible since $p > N$ by assumption.
Having now proven b has multiplicative order n modulo p, we must have $n \mid$ ______, which implies $p \equiv 1 \bmod n$, as desired. □

(e) Having completed the above setup, we now give the main argument of the proof. Suppose $p_1, \ldots, p_k$ are all the primes in $[1]_n$. Let $c = N!p_1 \cdots p_k$. Argue that there exists $M \in \mathbb{Z}$ large enough that $\Phi_n(Mc) > 1$.
Hint: what kind of function is $\Phi_n(x)$?
(f) Argue that $\Phi_n(Mc)$ must be coprime to c.
(g) Use the lemma and the previous part to argue that $\Phi_n(Mc)$ has no prime factors.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Factor $x^{20} - 1$ as a product of cyclotomic polynomials. Identify each factor as $\Phi_d(x)$ for some $d \mid 20$.

(H2) Show that if $n \geq 3$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.

(H3) Let $N = \Phi(n)$. Prove that the coefficients of $\Phi_n(x)$ are symmetric (that is, if we write

$$\Phi_n(x) = a_N x^N + a_{N-1}x^{N-1} + \cdots + a_1 x + a_0,$$

then $a_i = a_{N-i}$ for each i).

Hint: start by showing that $x^N \Phi_n(1/x)$ (i) is a polynomial, (ii) has the same coefficients as $\Phi_n(x)$ but in reverse order, and (iii) has the same complex roots as $\Phi_n(x)$.

(H4) Find a formula for $\Phi_n(1)$ in terms of n. Prove your formula holds.

Hint: your formula will likely depend on how many distinct prime factors n has.

(H5) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) For every $n \geq 3$, we have $\Phi_{2n}(x) = \Phi_n(-x)$.

(b) Every complex number on the unit circle in the complex plane is a root of some cyclotomic polynomial.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Find a formula for $\Phi_n(-1)$ in terms of n.