Math 461 **Spring 2020**
Homework 3 **Drew Armstrong**

Problem 1. Difference of nth Powers. Let $n \geq 1$ be a positive integer and let $\omega = e^{2\pi i/n}$. Prove that for all complex numbers $\alpha, \beta \in \mathbb{C}$ we have

$$\alpha^n - \beta^n = (\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta)\cdots(\alpha - \omega^{n-1}\beta).$$

Problem 2. Integral Domains. We say that a (commutative) ring R is an *integral domain* if for all $a, b \in R$ we have

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ or } b = 0.$$

The prototypical example is the ring of integers $\mathbb{Z}$, hence the name.

(a) Prove that a field is an integral domain.
(b) If R is integral domain, prove that $R[x]$ is integral domain. [Hint: Leading coefficients.]
(c) If $a, b, c \in R$ and $a \neq 0$ in an integral domain, prove that $ab = ac$ implies $b = c$.
(d) Consider any $a, b \in R$ with $a|b$ and $b|a$. In this case, use part (c) to show that $a = ub$ for some **invertible** element $u \in R$ (called a *unit*).

Problem 3. Bézout's Identity. Let $a, b \in \mathbb{Z}$ (not both zero) and consider the set

$$S = \{ax + by : x, y \in \mathbb{Z}, ax + by \geq 1\}.$$

By well-ordering this set contains a smallest elemement; call it $d \in S$.

(a) Prove that $d|a$ and $d|b$. [Hint: There exist $q, r \in \mathbb{Z}$ with $a = dq + r$ and $0 \leq r < d$. Show that $r \geq 1$ leads to a contradiction.]
(b) If $e|a$ and $e|b$ for some $e \in \mathbb{Z}$, show that $e|d$.

It follows that d is the *greatest common divisor* of a and b. In particular, we have shown that there exist some (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $\gcd(a, b) = ax + by$.

Problem 4. De Moivre's Formula.

(a) Use de Moivre's formula to express $\cos(2\theta)$ as a polynomial in $\cos\theta$.
(b) Solve this polynomial to obtain a formula for $\cos\theta$ in terms of $\cos(2\theta)$.
(c) Use your formula from (b) to obtain exact values for $\cos(\pi/2^n)$ when $n = 1, 2, 3, 4$.

Problem 5. Quadratic Formula Again.

(a) Find the two complex square roots of i. [Hint: Express i in polar form.]
(b) Use part (a) and the quadratic formula to solve the following equation for x:

$$x^2 + (2i)x + (-1 - i) = 0.$$

Problem 6. Cyclotomic Polynomials. We say that $\zeta \in \mathbb{C}$ is a *primitive nth root of unity* if $\zeta^n = 1$ and if $\zeta^k \neq 1$ for all $1 < k < n$. We define the *nth cyclotomic polynomial* as follows:

$$\Phi_n(x) := \prod(x - \zeta),$$

where ζ runs over the primitive nth roots of unity. By convention we say $\Phi_1(x) = x - 1$.

(a) Compute the polynomials $\Phi_2(x)$, $\Phi_4(x)$ and $\Phi_8(x)$. [Hint: Problem 5(a).]
(b) Prove that the polynomial $x^8 - 1 \in \mathbb{Q}[x]$ can be factored as follows:

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x).$$