ASSIGNMENT 7: COMP2711H

FALL 2015

Q1 Let p be a prime and $e \in \mathbb{N}$. Prove that $\phi(p^e) = (p-1)p^{e-1}$, where ϕ is Euler's totient function. (11 marks)

Q2 Let $m \geq 2$ and $n \geq 2$ be two positive integers with $\gcd(m,n) = 1$. Prove that $\phi(mn) = \phi(m)\phi(n)$. (12 marks)

Q3 Let $\mathbb{F}$ be a field. Prove that $(\mathbb{F}[x], +)$ is an abelian group with identity 0, called the zero polynomial, whose all coefficients are zero. (11 marks)

Q4 Let $R = \{a + b\sqrt{-1} \mid a, b \text{ integers }\}$. Prove that $(R, +, \cdot)$ is an integral domain. (11 marks)

Q5 Let $g \neq 0$ be a polynomial in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. Prove that for any $f \in \mathbb{F}[x]$ there exist unique polynomials $q, r \in \mathbb{F}[x]$ such that

$$f = qg + r,$$

where either $r = 0$ or $\deg(r) < \deg(g)$. (12 marks)

Q6 Let $f(x) = 2x^6 + x^3 + x^2 + 2 \in \mathrm{GF}(3)[x]$ and $g(x) = x^4 + x^2 + 2x \in \mathrm{GF}(3)[x]$. Use the Extended Euclidean Algorithm to find two polynomials u and v such that $\gcd(f,g) = uf + vg$.

Q7 Let $\mathbb{F}$ be a field. Let $m_1(x), m_2(x), \cdots, m_n(x)$ be pairwise coprime polynomials in $\mathbb{F}[x]$, where n is a positive integer. Prove that for any set of polynomials $a_1(x), a_2(x), \cdots, a_n(x)$ in $\mathbb{F}[x]$, the following system of congruences

$$u(x) \equiv a_i(x) \pmod{m_i(x)}, \quad i = 1, 2, \cdots, n$$

has exactly one solution modulo $M(x) = \prod_{i=1}^{n} m_i(x)$. Please give a constructive proof by showing a specific solution $u(x)$. (11 marks)

Q8 Solve the congruence $(x^2+1)f(x) \equiv 1 \pmod{x^3+1}$ in $\mathrm{GF}(3)[x]$, if possible. (11 marks)

Q9 Find out all irreducible polynomials of degree 3 over GF(2). (10 marks)

Date: Handed out on Nov. 13, due on Nov. 20 at the *beginning* of the lecture.