Fields and Coding Theory, MATH4109A/6101F — Fall 2013
Prof. Steven Wang — Carleton University

Homework Assignment #1
Due: Thursday, Oct. 10, 2013
Total marks: 90 /120. Term work: 10%

Instructions: Undergraduate students should do a combination of questions with a total of 90 marks. Graduate students should do a combination of questions with a total of 120 marks.

1. (10 Marks) Let $a(x) = x^9 + x^5 + x^3 + x + 1$, $b(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. First use Euclidean algorithm to compute $gcd(a(x), b(x))$ and then express it as a linear combination of $a(x)$ and $b(x)$ with polynomials in $\mathbb{F}_2[x]$ as coefficients.

2. (10 Marks) Let f be a quadratic or cubic polynomial over a field $\mathbb{F}$. Prove that if $f(\alpha) \neq 0$ for every $\alpha \in \mathbb{F}$ then f is irreducible over $\mathbb{F}$. Show that the result is not true if f has degree greater than or equal to 4.

3. (10 Marks) Prove that $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ has a multiple factor. Find all the factors of $f(x)$ and their multiplicities.

4. (15 Marks)

(a) Construct the addition and multiplication tables for $\mathbb{F}_3[x]/(x^2+1)$. Determine whether or not this ring is a field. (10 marks)

(b) Prove that for any finite field $\mathbb{F}_q$ of even characteristic, the ring $\mathbb{F}_q[x]/(x^9+x^5+x^3+x+1)$ cannot be a field. (5 marks)

5. (10 Marks) Consider a $(5, 2)$ linear code over $\mathbb{F}_2$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Determine all code words and the minimum distance of the code and then decode the vectors: $11111, 01101$ and 01100.

6. (10 Marks) Consider the binary encoding function that sends (a_1, a_2, a_3) into $(a_1, a_2, a_3, a_1 + a_2, a_2 + a_3, a_1 + a_3, a_1 + a_2 + a_3)$. First, give the generator matrix of this code. Then, provide the parity-check matrix, giving n, k and the minimum distance of the code. Finally, decode $m_1 = 1100010$ and $m_2 = 0111010$.

7. (10 Marks) Prove that the fields $\mathbb{F}_2[x]/(x^4+x+1)$ and $\mathbb{F}_2[x]/(x^4+x^3+x^2+x+1)$ are isomorphic.

8. (10 Marks) Show that $p(x) = x^3 - 2x - 2$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

9. (10 Marks) Show that $p(x) = x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Let θ be a root of $p(x)$. Compute $(1+\theta)(1+\theta+\theta^2+\theta^3)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{F}_2(\theta)$.

10. (10 Marks) Let $P = P(x_1, x_2, \cdots, x_n)$ be a polynomial in n variables over an arbitrary field $\mathbb{F}$. Suppose that the degree of P as a polynomial in x_i is at most t_i for $1 \le i \le n$, and let $S_i \subset \mathbb{F}$ be a set of at least $t_i + 1$ distinct members of $\mathbb{F}$. If $P(x_1, x_2, \cdots, x_n) = 0$ for all n-tuples $(x_1, x_2, \cdots, x_n) \in S_1 \times S_2 \times \cdots \times S_n$, then $P = 0$.

11. (10 Marks) Let p be a prime number. Prove that the cyclotomic polynomial $\Phi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$.

12. (15 Marks) Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ be the ring of Gauss integers, a subring of $\mathbb{C}$. Describe all elements of residue ring $R := \mathbb{Z}[i]/(3)$. Is R a field?

13. (10 Marks–Bonus) Let $x_1, \ldots, x_n$ be variables and $a_1, \ldots, a_n$ be nonnegative integers. Prove the constant term in the expansion of

$$\prod_{i \neq j} \left(1 - \frac{x_j}{x_i}\right)^{a_j}.$$

is the multinomial coefficient $\frac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}$. (Dyson's conjecture).