ASSIGNMENT 8: COMP2711H

FALL 2015

Q1 In the lecture about elementary number theory, we defined the congruence class mod p

$$\bar{i} = \{x \in \mathbb{Z} | x \equiv i \pmod{p}\},$$

where i is an integer and called *a representative* of its congruence class. Note that any integer in $\bar{i}$ can be employed as a representative of $\bar{i}$. We now define

$$\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{p-1}\}.$$

Define two binary operations on $\mathbb{Z}/p\mathbb{Z}$ as follows:

$$\bar{i} + \bar{j} = \overline{i+j} \text{ and } \bar{i} \times \bar{j} = \overline{ij}.$$

Let p be a prime.

(a) Prove that $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a finite field with p elements. (8 marks)

(b) Prove that $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is isomorphic to $(\mathbb{Z}_p, \oplus_p, \otimes_p)$. (8 marks)

Q2 Let $\pi(x) = x^2 + x + 2 \in \mathrm{GF}(3)[x]$.

(a) Prove that $\pi(x)$ is irreducible over GF(3). (3 marks)

(b) Write down all the elements in $\mathrm{GF}(3^2)$, where each element is a polynomial of degree at most one over GF(3). (3 marks)

(c) Let $\pi(x)$ be the irreducible polynomial for defining the multiplication in $\mathrm{GF}(3^2)$. Compute $(x+1) \cdot (2x+1)$. (3 marks)

(d) Find out the multiplicative inverse of $x+1$. (3 marks)

(e) Find out the minimal polynomial of $x+1$ over GF(3). (3 marks)

(f) Find out a generator α of $\mathrm{GF}(3^2)^*$, and express each α^i as a polynomial of degree at most 1 over GF(3). (3 marks)

(g) Compute $\mathrm{Tr}_{\mathrm{GF}(3^2)/\mathrm{GF}(3)}(x+1)$. (3 marks)

(h) Compute $\mathrm{N}_{\mathrm{GF}(3^2)/\mathrm{GF}(3)}(x+1)$. (3 marks)

Q3 Show that the sum of all elements in $\mathrm{GF}(p^m)$ is zero, if $p^m \neq 2$. (12 marks)

Q4 Let $\mathbb{F} = \mathrm{GF}(q^n)$ and $\mathbb{K} = \mathrm{GF}(q)$. Prove the following properties of the trace function $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x)$ from $\mathbb{F}$ to $\mathbb{K}$:

(a) $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a+b) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a) + \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(b)$ for all $a, b \in \mathbb{F}$. (4 marks)

(b) $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(ca) = c\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$ for all $a \in \mathbb{F}$ and $c \in \mathbb{K}$. (4 marks)

(c) $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(c) = nc$ for all $c \in \mathbb{K}$. (4 marks)

(d) $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a^q) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(a)$. (4 marks)

Q5 Let $\mathbb{K} = \mathrm{GF}(q)$ and $\mathbb{F} = \mathrm{GF}(q^n)$. Prove the following properties of the norm function $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x)$:

(a) $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(ab) = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)\mathrm{N}_{\mathbb{F}/\mathbb{K}}(b)$ for all $a, b \in \mathbb{F}$. (4 marks)

(b) $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a) = a^n$ for all $a \in \mathbb{K}$. (4 marks)

(c) $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(a^q) = \mathrm{N}_{\mathbb{F}/\mathbb{K}}(a)$ for all $a \in \mathbb{F}$. (4 marks)

Q6 Let $f(x) = x^d + b_{d-1}x^{d-1} + \cdots + b_1 x + b_0 \in \mathrm{GF}(p)[x]$ be the minimal polynomial of $\beta \in \mathrm{GF}(p^m)$ over $\mathrm{GF}(p)$. Prove that

$$\mathrm{Tr}_{\mathrm{GF}(p^m)/\mathrm{GF}(p)}(\beta) = -(m/d)b_{d-1}$$

and

$$\mathrm{N}_{\mathrm{GF}(p^m)/\mathrm{GF}(p)}(\beta) = (-)^m b_0^{m/d}.$$

(20 marks)

Date: Handed out on Nov. 25, due on Dec. 2 (Please give your assignment paper to the TA between 3:30pm-4:30pm on Dec. 2, his office is at Room 2394).