Fields and Coding Theory, MATH4109/6101 Fall 2013
Prof. Steven Wang Carleton University

Homework Assignment #2
Due: Thursday, Nov. 14, 2013
Total marks: 100/120. Term work: 10%

Instruction: Undergraduate students should only do 8 questions including questions 1, 2, 8, 9 and any other four questions of your choices. Graduate student should do all 10 questions.

1. (15 Marks) Consider the field $\mathbb{F}_{47}$.

(i) Compute $ord(2)$ and $ord(3)$ in the multiplicative group $\mathbb{F}_{47}^*$.

(ii) Use Gauss algorithm to find a primitive element of $\mathbb{F}_{47}$.

(iii) Find the least primitive element g of $\mathbb{F}_{47}$, i.e., g is a primitive element, $0 < g < 46$, and $g \leq h$ for any primitive element h with $0 < h < 46$.

2. (15 Marks)

(i) Prove that $x^3 + 2x^2 + 1$ is irreducible over $\mathbb{F}_3$.

(ii) Determine a primitive element γ of $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3 + 2x^2 + 1)$.

(iii) Express all nonzero elements of $\mathbb{F}_{27}$ as powers of the primitive element.

(iv) Find the smallest positive integer k such that $\gamma^3 + \gamma^7 = \gamma^k$.

3. (10 Marks) Let q be a prime power and r be a prime divisor of $q - 1$. Let $a \in \mathbb{F}_q^*$ and $ord(a) = m > 1$ in $\mathbb{F}_q^*$. Prove that $r \mid (q-1)/m$ if and only if $a \in \mathbb{F}_q^{*r}$.

4. (10 Marks) Prove that for any positive integer m,

$$\sum_{a \in \mathbb{F}_q} a^m = \begin{cases} -1, & \text{if } (q-1) \mid m \\ 0, & \text{otherwise.} \end{cases}$$

5. (10 Marks) Let $a(n)$ and $b(n)$ be functions defined on the set of positive integers with values in a multiplicative group G, and assume that G is abelian. Prove that

$$b(n) = \prod_{d \mid n} a(d)$$

if and only if

$$a(n) = \prod_{d|n} b(d)^{\mu(\frac{n}{d})}.$$

This is the multiplicative version of Möbius inversion formula.

6. (10 Marks) From Question 5 and the following formula that we covered in the class

$$x^{q^n} - x = \prod_{d|n} \Phi_{q,d}(x),$$

deduce the following formula

$$\Phi_{q,n}(x) = \prod_{d|n} (x^{q^d} - x)^{\mu(\frac{n}{d})}, \tag{1}$$

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the prime factorization of n. Using (1), prove that

$$n\Phi_{q,n} = q^n - \sum_{i=1}^{r} q^{n/p_i} + \sum_{1 \le i < j \le r} q^{n/p_i p_j} + \cdots + (-1)^r q^{n/p_1 \cdots p_r}.$$

7. (10 Marks) Let q be a power of an odd prime. Prove that an element $\alpha \in \mathbb{F}_q^*$ is a square element of $\mathbb{F}_q^*$ if and only if $\alpha^{(q-1)/2} = 1$. In particular, $-1 \in \mathbb{F}_q^{*2}$ if and only if $q \equiv 1 \pmod 4$.

8. (20 Marks) Consider $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$.

(i) Compute all characteristic polynomials over $\mathbb{F}_2$ of elements of $\mathbb{F}_{16}$.

(ii) Compute all minimal polynomials over $\mathbb{F}_2$ of elements of $\mathbb{F}_{16}$ and point out the primitive ones.

9. (10 Marks) Factor $x^{64} - x^4$ into irreducible factors:

(i) over $\mathbb{F}_{16}$.

(ii) over $\mathbb{F}_4$.

(iii) over $\mathbb{F}_2$.

10. (10 Marks) Let q be a power of an odd prime. Prove that

$$x^{(q-1)/2} - 1 = \prod_{\alpha \in \mathbb{F}_q^{*2}} (x - \alpha), \quad x^{(q-1)/2} + 1 = \prod_{\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}} (x - \alpha).$$

Then deduce that for any $f(x) \in \mathbb{F}_q[x]$ which can be completely factored into distinct linear factors and $f(0) \neq 0$, let

$$g(x) = gcd(f(x), x^{(q-1)/2} - 1),$$

then $g(x)$ is a proper divisor of $f(x)$ if and only if $f(x)$ has at least one root in $\mathbb{F}_q^{*2}$ and at least one root in $\mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.