

MATH 291T**Homework 4**

Due on Thursday 03/19/09

1. It is given that $f(x) = x^4 + x + 1$ is irreducible and primitive over $GF(2)$. Define α by $f(\alpha) = 0$.
- (a) Set up a table for $GF(16)$ containing the binary, exponential and polynomial representation of every element in $GF(16)$.
- (b) Solve for x and y : $\begin{cases} x + \alpha^7 y = \alpha^{10} \\ \alpha^2 x + y = \alpha^5 \end{cases}$. Write all elements of $GF(16)$ in exponential form.
- (c) Find the quotient and remainder of $x^5 + \alpha^2 x^4$ divided by $x^2 + \alpha x + \alpha^2$. Write all elements of $GF(16)$ in exponential form.

2. Let β be a primitive 5-th root of unity in $GF(16)$. Then over $GF(16)$, we can factor $x^5 - 1$ as

$$x^5 - 1 = (x - 1)(x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

Let α be defined as in Exercise 1. Write all elements of $GF(16)$ in exponential form.

- (a) What are the choices for β in terms of α ?
- (b) Use cyclotomic cosets to find the degrees of the irreducible factors of $x^5 - 1$ over $GF(2)$.
- (c) Use the table from Exercise 1 to expand the appropriate combinations of $x - 1$, $x - \beta$, $x - \beta^2$, $x - \beta^3$ and $x - \beta^4$ to get the irreducible factors of $x^5 - 1$ over $GF(2)$.
- (d) We can view $GF(4)$ as a subfield of $GF(16)$. Which elements of $GF(16)$ form $GF(4)$?
- (e) Use cyclotomic cosets to find the degrees of the irreducible factors of $x^5 - 1$ over $GF(4)$.
- (f) Use the table from Exercise 1 to expand the appropriate combinations of $x - 1$, $x - \beta$, $x - \beta^2$, $x - \beta^3$ and $x - \beta^4$ to get the irreducible factors of $x^5 - 1$ over $GF(4)$.
3. This exercise is about the ‘Squaring Rule’ in characteristic 2.
- (a) Let $a, b \in GF(2^n)$. Prove that $(a + b)^2 = a^2 + b^2$.
- (b) Let $a_1, \dots, a_k \in GF(2^n)$. Prove that $(a_1 + a_2 + \dots + a_k)^2 = a_1^2 + a_2^2 + \dots + a_k^2$.
- (c) Let $f(x)$ be a polynomial over $GF(2)$. Prove that α^2 is a root of $f(x)$ if α is a root of $f(x)$.
-
-