

Homework 2
MATH3807/COMP3807 Mathematical Software
Winter 2010 – Due on 7 April

(1) (20 marks)

(a) (10 marks) Using interpolation, give a polynomial $f \in \mathbb{F}_{11}[x]$ of degree at most 3 satisfying

$$f(0) = 2, \quad f(2) = 3, \quad f(3) = 1, \quad f(7) = 6$$

(b) (10 marks) What are all the polynomials in $\mathbb{F}_{11}[x]$ which satisfy $f(0) = 2, f(2) = 3, f(3) = 1, f(7) = 6$?

(2) (20 marks) Hand in your completed worksheets from labs “Fast Multiplication” and “Fast Multiplication II”. Hand it in to me by saving the worksheet to a file (after making sure all the cells you want are evaluated) and then emailing it to me.

(3) (20 marks) Let \mathbb{F} be a field and $a(x) \in \mathbb{F}[x]$ be a polynomial of degree $n - 1 = 3^k - 1$.

(a) (5 marks) Show that $a(x)$ can be decomposed into

$$a(x) = b(x^3) + x \cdot c(x^3) + x^2 \cdot d(x^3),$$

where $b(x), c(x)$ and $d(x)$ are polynomials in $\mathbb{F}[x]$ of degree at most $n/3 - 1 = 3^{k-1} - 1$.

(b) (5 marks) Show that if $\omega \in \mathbb{F}$ is a primitive n th root of unity, then $a(x)$ can be evaluated at all the powers of ω by recursively evaluating $b(x), c(x)$ and $d(x)$ at the powers of ω^3 .

(c) (5 marks) Put all of this together into an algorithm similar to FFT for evaluating $a(x)$ at the powers of ω .

(d) (5 marks) What are the number of additions and number of multiplications in \mathbb{F} that this algorithm does on input size n ?

(e) (bonus 10 marks) The set $S = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ has some special properties that make this “3-ary” FFT (and the “binary” FFT from class) work. What properties does a set S need to be used in this way (or in the original FFT algorithm)? Can you find any other sets that have these properties?

(4) (20 marks) Consider the following two polynomials in $\mathbb{F}_{17}[x]$

$$f(x) = 7x^3 + 15x + 1 \qquad g(x) = 16x^4 + 5x^3 + 13x + 1$$

(a) (10 marks) Use Karatsuba’s algorithm, by hand, to multiply these two polynomials.

(b) (10 marks) Use the FFT algorithm, by hand, to multiply these two polynomials.

(5) (20 marks) Remember that if a polynomial has degree 3 or less then it is irreducible if and only if it has at least one linear factor, that $(x - a)$ is a linear factor of a polynomial $f(x)$ if and only if $f(a) = 0$ and that for small fields it is easy to check by hand if a particular value is a root of a polynomial.

(a) (10 marks) Which of the following polynomials are reducible and irreducible in $\mathbb{F}_5[x]$? What is the factorization of the reducible ones?

$$m_0 = x^3 + 3, \quad m_1 = x^2 + 3x + 1, \quad m_2 = x^2 + 3, \quad , m_3 = x^3 + 3x^2 + 2x + 1.$$

(b) (10 marks) Does the following system have a unique solution of smallest degree:

$$f \equiv 3x + 1 \pmod{m_0} \qquad f \equiv 3 \pmod{m_2}$$

Why or why not? If yes, what is that solution?