Foundations of Computer Algebra. CS424b: Quiz 2. UWO, March 8, 2006.

Student ID number:
Student Last Name:

Guidelines. Every printed document is allowed but computers and calculators are not. The duration of the quiz is 40 minutes. The quiz consists of two exercises located on pages 2 and 4.. All answers should be written in the *answer boxes*. No justifications for the answers are needed, unless explicitly required. You are expected to do this quiz on your own without assistance from anyone else in the class. If possible, please avoid pencils and use pens with dark ink. Thank you.

Notations. The set of non-negative integer numbers, integer numbers and rational numbers are denoted respectively $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, as usual. For an integer $n \in \mathbb{Z}$ the set of the multiples of n (all of them: positive, null or negative) is denoted by $n\mathbb{Z}$. For an integer $n \in \mathbb{Z}$ the residue class ring of the binary relation $(a, b) \longmapsto a \equiv b \mod n$ is denoted by $\mathbb{Z}/n\mathbb{Z}$, as usual. For a ring $\mathbb{A}$, we denote by $\mathbb{A}[x]$ the ring of univariate polynomials in x with coefficients in $\mathbb{A}$.

Formulas. We give the mutiplication table of $\mathbb{Z}/17\mathbb{Z}$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Exercise 1. In this exercise, detailed and precise explanations are required. As expected, we consider the field $\mathbb{K} = \mathbb{Z}/17\mathbb{Z}$.

1. Show that 3 is in $\mathbb{K}$ a primitive 16-th root of unity.
2. Find all primitive 4-th roots of unity in $\mathbb{K}$.

Answer 1

Answer 2

Exercise 2. In the ring $\mathbb{A} = \mathbb{K}[x]$ of univariate polynomials with coefficients in $\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$, we consider the polynomials $f_1 = x^2 + x + 1$, $f_2 = x + 1$, $f_3 = x^3 + x^2 + x + 1$.

For every pair (f_i, f_j), with $1 \leq i < j \leq$ such that we can compute the product $f_i f_j$ by means of the FFT-based algorithm studied in class:

1. find a suitable primitive n-th root of unity in $\mathbb{K}$,
2. compute the DFT of f_1 and f_j
3. deduce the product of the polynomials f_i and f_j by means of the FFT-based algorithm studied in class

Answer 3

Answer 4

Answer 5

Answer 6