

Арифметические алгоритмы и продвинутое структуры данных. Домашняя работа №2.

Часть 1. Выберите неприводимый многочлен $f \in \mathbb{Z}_2[x]$ степени $n: 2 \leq n \leq 64$. В дальнейшем все операции выполняются по этому модулю.

1. Напишите функцию, представляющую элемент из $GF(2^n)$ в полиномиальной форме и наоборот.
2. Напишите функцию, умножающую два произвольных двоичных многочлена степени не выше 32.
3. Напишите функцию умножения двух элементов из $GF(2^n)$. При выводе продемонстрируйте результаты для различных неприводимых многочленов, с помощью которых определяется операция умножения.
4. Реализуйте расширенный алгоритм Евклида для $GF(2^n)$.
5. Напишите функцию, которая ищет мультипликативный обратный для элемента из $GF(2^n)$.

Часть 2.

1. Von zur Gathen Modern Computer Algebra: 8 Fast multiplication 235 p.: № 8.1 (**Prog**), 8.13, 8.14, 8.24 (**Prog**).
2. Кормен и др. Алгоритмы: построение и анализ. 948 стр.: № 30.1.6, 30.1.7 (**Prog**); 957 стр. №30.2.5; стр. 964: №30.3 (**Prog**).
3. Д. Кнут. Искусство программирования. Т. 2. Раздел 4.3.3 упр. 9; Раздел 4.6.4 упр. 41 (**Prog**).