1 Конечнозначные функции.

2 Группы. Теория Пойа.

3 Конечные поля.

3.1. Поделить с остатком многочлен $f(x) \in \mathbb{Z}_p[x]$ на многочлен $g(x) \in \mathbb{Z}_p[x]$, если

1) $p = 2$, $f(x) = x^3 + x + 1$, $g(x) = x + 1$;
2) $p = 2$, $f(x) = x^4 + x^2 + x$, $g(x) = x^2 + x + 1$;
3) $p = 2$, $f(x) = x^4 + 1$, $g(x) = x^2 + 1$;
4) $p = 2$, $f(x) = x^5 + x^4 + x^2$, $g(x) = x^3 + x + 1$;
5) $p = 3$, $f(x) = 2x^2 + x + 2$, $g(x) = x + 2$;
6) $p = 3$, $f(x) = x^3 + 2x^2 + x + 2$, $g(x) = x^2 + 2$;
7) $p = 5$, $f(x) = 4x^2 + 3x + 2$, $g(x) = 3x + 2$;
8) $p = 5$, $f(x) = 3x^3 + 4x^2 + 2x + 1$, $g(x) = 2x^2 + 3$.

3.2. Найти наибольший общий делитель $f(x) \in \mathbb{Z}_p[x]$ многочленов $f_1(x), f_2(x) \in \mathbb{Z}_p[x]$, если

1) $p = 2$, $f_1(x) = x^4 + x^2 + 1$, $f_2(x) = x^2 + 1$;
2) $p = 2$, $f_1(x) = x^6 + x^5 + x^4 + 1$, $f_2(x) = x^5 + x + 1$;
3) $p = 2$, $f_1(x) = x^7 + 1$, $f_2(x) = x^5 + x^3 + x + 1$;
4) $p = 3$, $f_1(x) = x^3 + 1$, $f_2(x) = 2x^2 + x + 2$;
5) $p = 3$, $f_1(x) = x^4 + x^2 + x + 2$, $f_2(x) = x^2 + 2$;
6) $p = 3$, $f_1(x) = x^8 + 2x^5 + x^3 + x^2 + 1$, $f_2(x) = 2x^6 + x^5 + 2x^3 + 2x^2 + 2$;
7) $p = 5$, $f_1(x) = x^2 + 1$, $f_2(x) = x^2 + 4x + 3$;
8) $p = 5$, $f_1(x) = x^3 + 4x + 1$, $f_2(x) = x^2 + x + 3$.

3.3. Выяснить, является ли многочлен $f(x) \in \mathbb{Z}_p[x]$ неприводимым над полем $\mathbb{Z}_p$, если

1) $p = 2$, $f(x) = x^2 + 1$;
2) $p = 2$, $f(x) = x^3 + x + 1$;
3) $p = 2$, $f(x) = x^4 + x + 1$;
4) $p = 2$, $f(x) = x^4 + x^2 + 1$;
5) $p = 3$, $f(x) = x^2 + 1$;
6) $p = 3$, $f(x) = x^3 + 2x + 2$;
7) $p = 3$, $f(x) = x^4 + 2$;

8) $p = 5$, $f(x) = x^3 + 2x^2 + 3x + 1$.

3.4. Найти все неприводимые многочлены $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_p[x]$, где $a_n = 1$, над полем $\mathbb{Z}_p$, если

1) $p = 2$, $n = 2$;
2) $p = 2$, $n = 3$;
3) $p = 2$, $n = 4$, $a_0 = 1$;
4) $p = 2$, $n = 4$, $a_3 = 0$;
5) $p = 3$, $n = 2$;
6) $p = 3$, $n = 3$, $a_0 = 1$;
7) $p = 5$, $n = 2$, $a_1 = 1$;
8) $p = 5$, $n = 2$, $a_0 = 2$.

3.5. Выяснить, является ли кольцо $\mathbb{Z}_p[x]/(f)$ полем, если

1) $p = 2$, $f(x) = x^3 + x + 1$;
2) $p = 2$, $f(x) = x^4 + x + 1$;
3) $p = 3$, $f(x) = x^3 + 2x + 1$;
4) $p = 3$, $f(x) = x^4 + x + 2$.

3.6. Найти сумму и произведение элементов g_1 и g_2 в кольце $\mathbb{Z}_p[x]/(f)$, если

1) $p = 2$, $f(x) = x^3 + x^2 + 1$, $g_1(x) = x^2$, $g_2(x) = x + 1$;
2) $p = 2$, $f(x) = x^4 + x^3 + 1$, $g_1(x) = x^3 + x^2$, $g_2(x) = x^3 + 1$;
3) $p = 2$, $f(x) = x^5 + x^2 + 1$, $g_1(x) = x^4 + x^2 + 1$, $g_2(x) = x^3 + x + 1$;
4) $p = 2$, $f(x) = x^5 + x^4 + x^3 + x + 1$, $g_1(x) = x^4$, $g_2(x) = x^3 + x^2 + x + 1$;
5) $p = 3$, $f(x) = x^4 + x^2 + 1$, $g_1(x) = x^3 + 2x + 2$, $g_2(x) = 2x^2 + 1$;
6) $p = 3$, $f(x) = x^4 + x + 2$, $g_1(x) = x^3 + 2x^2 + 1$, $g_2(x) = x^2 + 2x$;
7) $p = 5$, $f(x) = x^3 + x^2 + 2$, $g_1(x) = x^2 + 4x + 3$, $g_2(x) = 3x^2 + 2x + 1$;
8) $p = 5$, $f(x) = x^3 + 3x + 2$, $g_1(x) = x^2 + 3x + 4$, $g_2(x) = x^2 + 2$.

Является ли это кольцо полем?

3.7. Построить таблицы сложения и умножения элементов в поле из p^n элементов, если

1) $p = 2$, $n = 2$;
2) $p = 2$, $n = 3$;
3) $p = 3$, $n = 2$;
4) $p = 2$, $n = 4$.

3.8. По алгоритму Евклида найти обратный элемент к элементу a в поле $\mathbb{Z}_p$, если

1) $p = 7$, $a = 4$;
2) $p = 11$, $a = 9$;
3) $p = 13$, $a = 5$;
4) $p = 17$, $a = 13$;
5) $p = 19$, $a = 15$;
6) $p = 23$, $a = 16$;
7) $p = 29$, $a = 17$;
8) $p = 31$, $a = 27$.

3.9. По алгоритму Евклида найти обратный элемент к элементу g в поле $\mathbb{Z}_p[x]/(f)$, если

1) $p = 2$, $f(x) = x^3 + x^2 + 1$, $g(x) = x^2$;
2) $p = 2$, $f(x) = x^4 + x + 1$, $g(x) = x^2 + x + 1$;
3) $p = 2$, $f(x) = x^4 + x^3 + x^2 + x + 1$, $g(x) = x^3 + 1$;
4) $p = 2$, $f(x) = x^5 + x^3 + 1$, $g(x) = x^2 + x + 1$;
5) $p = 3$, $f(x) = x^3 + 2x + 1$, $g(x) = x + 2$;
6) $p = 3$, $f(x) = x^4 + 2x^2 + 2$, $g(x) = x^2 + x + 2$;
7) $p = 5$, $f(x) = x^3 + x^2 + 1$, $g(x) = x^2 + 4x + 3$;
8) $p = 5$, $f(x) = x^4 + 3x^2 + x + 1$, $g(x) = x^2 + 2x + 3$.

3.10. Найти примитивный элемент поля $\mathbb{Z}_p$, если

1) $p = 7$;
2) $p = 11$;
3) $p = 13$;
4) $p = 17$;
5) $p = 19$;
6) $p = 23$;
7) $p = 29$;
8) $p = 31$.