Волкова. Вариант 1

1) Найти все подгруппы группы 1.1) $\mathbb{Z}_{33}^{+}$:

1: $\{0, 1, 2, \dots, 32\}$

3: $\{0, 3, 6, 9, \dots, 30\}$

11: $\{0, 11, 22\}$

33: $\{0\}$

2) Перечислить все элементы группы $\mathbb{Z}_n^{*}$. Вычислить их порядок. Какие из них явл. генераторами группы?

2.1) $n = 10$

$\{1, 3, 7, 9\}$

порядок 1 : 1 $(1^1 = 1)$

3 : 4 $(3^1 = 3, 3^2 = 9, 3^3 = 7, 3^4 = 1)$

7 : 4 $(7^1 = 7, 7^2 = 9, 7^3 = 3, 7^4 = 1)$

9 : 2 $(9^1 = 9, 9^2 = 1)$

генераторы : 3; 7

$n = 11$

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

порядок 1 : 1 $(1^1 = 1)$

2 : 10 $(2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1)$

3 : 5 $(3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1)$

4 : 5 $(4^1 = 4, 4^2 = 5, 4^3 = 9, 4^4 = 3, 4^5 = 1)$

5 : 5 $(5^1 = 5, 5^2 = 3, 5^3 = 4, 5^4 = 9, 5^5 = 1)$

6 : 10 $(6^1 = 6, 6^2 = 3, 6^3 = 7, 6^4 = 9, 6^5 = 10, 6^6 = 5, 6^7 = 8, 6^8 = 4, 6^9 = 2, 6^{10} = 1)$

7 : 10 $(7^1 = 7, 7^2 = 5, 7^3 = 2, 7^4 = 3, 7^5 = 10, 7^6 = 4, 7^7 = 6, 7^8 = 9, 7^9 = 8, 7^{10} = 1)$

8 : 10 $(8^1 = 8, 8^2 = 9, 8^3 = 6, 8^4 = 4, 8^5 = 10, 8^6 = 3, 8^7 = 2, 8^8 = 5, 8^9 = 7, 8^{10} = 1)$

9 : 5 $(9^1 = 9, 9^2 = 4, 9^3 = 3, 9^4 = 5, 9^5 = 1)$

10 : 2 $(10^1 = 10, 10^2 = 1)$

генераторы : 2; 6; 7; 8

3) Используя теорему Лагранжа, найти 3.1) $3^{452} \bmod 11$

$3^{452 \bmod 5} \bmod 11 = 3^2 \bmod 11 = 9$ Ответ: 9

4) В кольце $F_2[x]$ вычислить $x^4 + x + 1 \bmod x^3 + x + 1$

$$\begin{array}{r|l} x^4 + x + 1 & x^3 + x + 1 \\ \hline x^4 + x^2 + x & x \\ \hline x^2 + 1 & \end{array}$$

Ответ: $x^2 + 1$

5) В кольце $F_2[x]$ вычислить $(x^4 + x)(x^2 + x + 1) \bmod x^4 + x + 1$

$(x^4 + x)(x^2 + x + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x$

$$\begin{array}{r|l} x^6 + x^5 + x^4 + x^3 + x^2 + x & x^4 + x + 1 \\ \hline x^6 + x^3 + x^2 & x^2 + x + 1 \\ \hline x^5 + x^4 + x & \\ x^5 + x^2 + x & \\ \hline x^4 + x^2 & \\ x^4 + x + 1 & \\ \hline x^2 + x + 1 & \end{array}$$

Ответ: $x^2 + x + 1$

6) Является ли каждое из этих множеств полем или кольцом с операциями сложения, умножения по соответствующему модулю?

$\mathbb{Z}_{31}$ = поле, т.к. 31 - простое число

$\mathbb{Z}_{28}$ – кольцо, т.к. 2, 4, 7, 14 – делители нуля

7) Являются ли эти расширения поле кольцом или полем?

$GF(3)/\langle x^2+2\rangle$ – кольцо, т.к. $x^2+2 = (x+1)(x+2) = x^2+\underbrace{x+2x}_{0x}+2$
(есть делит. нуля)

$GF(2)/\langle (x^3+x+1)^2\rangle$ – кольцо, т.к. $(x^3+x+1)^2 = (x^3+x+1)(x^3+x+1)$ –
есть делит. нуля

$GF(2)/\langle x^3+x+1\rangle$ – поле, т.к. x^3+x+1 не им. корней $\Rightarrow$ нет делит. нуля

8) Пусть в группе G: $\forall a \in G \mid a*a=e$, Доказать, что группа G абелева.

Д-во: $a*e*a = (a*e)*a = a*a = e$

$e = a*e*a = a*(b*b)*a = (a*b)*(b*a)$

$a*b = a*b*e = (a*b)*((b*a)*(b*a)) = ((a*b)*(b*a))*(b*a) = e*(b*a) = b*a$

$\Rightarrow a*b = b*a \Rightarrow$ группа абелева.

9) Дан примитивный над GF(2) полином $p(x) = x^3+x+1$.
Пусть α – примитивный элемент поля $GF(2^3) = F_2[x]/\langle p(x)\rangle$, равный полиному x. Тогда $\alpha^2 = x^2$; $\alpha^3 = x^3 = c_2x^2+c_1x+c_0 \bmod p(x)$
$c_i \in GF(2)$; и т.д. Найти n!

9.1) $\alpha^5+\alpha^3 = \alpha^n$

$\alpha^5 = \alpha^2\cdot\alpha^3 = x^2(x+1) = x^3+x^2 = x+1+x^2$

$\alpha^3 = x+1$

$\alpha^5+\alpha^3 = x+1+x^2+x+1 = x^2 = \alpha^2$ Ответ: n=2

10) $g(x) = x^8+x^4+x^3+x^2+1$ – мин. полином над GF(2)
Пусть один байт $(b_7 \dots b_0)$ – коэфф. полинома из $GF(256) = GF(2)[x]/\langle g(x)\rangle$. Числа записаны в кодировке big endian.
Преобразовать числа в полиномы, вост. оп. в поле GF(256), получить полином – элемент поля GF(256) и прообр. его в число.

10.1) 128·6+29

$128_{10} = 1000.0000_2$: x^7 (7 6 5 4 3 2 1 0)

$6_{10} = 0000.0110_2$: x^2+x

$29_{10} = 0001\,1101_2$: $x^4+x^3+x^2+1$

$x^7(x^2+x)+x^4+x^3+x^2+1 = x^8\cdot x + x^8 + x^8 = (x^4+x^3+x^2+1)\cdot 0 =$

$= x^5+x^4+x^3+x$: $00111010_2 = 32+16+8+2_{10} = 58_{10}$

Ответ: 58