1. **Условие:** Найти все подгруппы группы Z_{33}^+.

   Решение: По теореме Лагранжа порядок любой подгруппы конечной группы является делителем порядка группы. Так что подгруппами группы Z_{33}^+ будут группы $\{0\}, \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}, \{0, 11, 22\}, Z_{33}^+$.

2. **Условие.:** Перечислить все элементы группы Z_n^*. Вычислить их порядок. Какие из них являются генераторами группы?

   а) $n = 10$.

   б) $n = 11$.

   Решение:

   а) $Z_{10}^* = \{1, 3, 7, 9\} =< 3 >=< 7 >$.

g - элемент	1	3	7	9
ord g	1	4	4	2

   б) $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} =< 2 >=< 6 >=< 7 >=< 8 >$.

g - элемент	1	2	3	4	5	6	7	8	9	10
ord g	1	10	5	5	5	10	10	10	5	2

3. **Условие:** Используя теорему Лагранжа, найти $3^{452} mod\ 11$.

   Решение: $3^{452} mod\ 11 = 3^{41*11+1} mod\ 11 = 3$

4. **Условие:** В кольце $F_2[x]$ вычислить $x^4 + x + 1\ mod\ x^3 + x + 1$

   Решение:

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

   $x^4 + x + 1\ mod\ x^3 + x + 1 = x^2 + 1$

5. **Условие:** В кольце $F_2[x]$ вычислить $(x^4 + x)(x^2 + x + 1)\ mod\ x^4 + x + 1$

   Решение:

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

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + x & x^4 + x + 1 \\ \cline{2-2}
\underline{x^6 + x^3 + x^2} & x^2 + x + 1 \\
\quad x^5 + x^4 + x & \\
\quad \underline{x^5 + x^2 + x} & \\
\qquad x^4 + x^2 & \\
\qquad \underline{x^4 + x + 1} & \\
\qquad\quad x^2 + x + 1 &
\end{array}
$$

$(x^4 + x)(x^2 + x + 1) \ mod \ x^4 + x + 1 = x^2 + x + 1$

6. **Условие:** Является ли каждое из этих множеств полем или кольцом с операциями сложения, умножения по соответствующему модулю?

   а) Z_{31}.

   б) Z_{28}.

   Решение:

   а) Z_{31} — порядок 31 это простое число, следовательно для любого элемента по умножению будет существовать обратный. По сложению абелева группа. Следовательно это поле.

   б) Z_{28} — рассуждаем аналогично случаю Z_{31}, только 28 это составное число. Следовательно это кольцо.

7. **Условие:** Являются ли эти расширение поля кольцом или полем?

   а) $GF(3)/ < x^2 + 2 >$.

   б) $GF(2)/ < (x^3 + x + 1)^2 >$.

   в) $GF(2)/ < x^3 + x + 1 >$.

   Решение:

   а) $GF(3)/ < x^2 + 2 >$ — $x^2 + 2 = (x + 2)(x + 1)$. В множестве есть делители нуля, следовательно оно не является полем, то есть это кольцо.

   б) $GF(2)/ < (x^3 + x + 1)^2 >$ — $(x^3 + x + 1)^2 = (x^3 + x + 1)(x^3 + x + 1)$. Следовательно не может быть полем, то есть это кольцо.

   в) $GF(2)/ < x^3 + x + 1 >$ — $x^3 + x + 1$ в $GF(2)$ неприводим. Следовательно это поле.

8. **Условие:** Пусть в группе $G\colon \forall a \in G\ a * a = e$. Доказать, что группа G абелева. Указание: использовать тот факт, что $a * e * a = e$.

   Решение: Для того, чтобы доказать, что группа G абелева, необходимо показать, что она комутативна, то есть $\forall a, b \in G\ a * b = b * a$.

   $a * e * a = a * (b * e * b) * a = (a * b) * e * (b * a) = e \Rightarrow (a * b) * (b * a) * (b * a) = (b * a) \Rightarrow a * b = b * a$, ч.т.д.

9. **Условие:** Дан примитивный над $GF(2)$ полином $p(x) = x^3 + x + 1$. Пусть α — примитивный элемент поля $GF(2^3) = F_2[x]/ < p(x) >$, равный полиному x. Тогда $\alpha^2 = x^2$; $\alpha^3 = x^3 \equiv c_2x^2 + c_1x + c_0\ mod\ p(x), c_i \in GF(2)$; и т.д. Найти $n\colon \alpha^5 + \alpha^3 = \alpha^n$.

   Решение:
   $\alpha^3 = x^3\ mod\ x^3 + x + 1 = x + 1$
   $\alpha^5 = x^5\ mod\ x^3 + x + 1 = x^2 + x + 1$
   $\alpha^3 + \alpha^5 = x^2 \Rightarrow n = 2$

10. **Условие:** $g(x) = x^8 + x^4 + x^3 + x^2 + 1$ — минимальный полином над $GF(2)$.
    Пусть один байт (восемь бит $b_7...b_0$) — это коэффициенты полинома $b_7x_7 + ... + b_0$ из $GF(256) = GF(2)[x]/ < g(x) >$.
    Числа записаны в кодировке big endian, например $32 \leftrightarrow 00100000$.
    Преобразовать числа в полиномы, выполнить операции в поле $GF(256)$, получить полином — элемент поля $GF(256)$ и преобразовать его в число. Это число является ответом задачи. Использовать тот факт, что $x^8 \equiv x^4 + x^3 + x^2 + 1\ mod\ g(x)$.
    Найти $128 * 6 + 29$.

    Решение:
    $128_{10} = 10000000_2 = x^8\ mod\ x^8 + x^4 + x^3 + x^2 + 1 = x^4 + x^3 + x^2 + 1$
    $6_{10} = 110_2 = x^2 + x$
    $29_{10} = 11101_2 = x^4 + x^3 + x^2 + 1$
    $128 * 6 + 29 = (x^4 + x^3 + x^2 + 1) * (x^2 + x) + x^4 + x^3 + x^2 + 1 = x^6 + x^5 + x^4 + x^2 + x^5 + x^4 + x^3 + x + x^4 + x^3 + x^2 + 1 = x^6 + x^4 + x + 1 = 1010011_2 = 83_{10}$