ДОМАШНЯ РОБОТА №7
З ПРЕДМЕТУ
"МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ"

ФІ-12 Бекешева Анастасія

1. У кільці поліномів над полем кожен ненульовий елемент є оберненим, тобто кожен елемент можна ділити на будь-який ненульовий елемент з лишком. У кільці поліномів над кільцем (навіть цілісним) це не виконується. Наявність обернених елементів у кільці є необхідною, але не достатньою умовою для того, щоб будь-який елемент можна було поділити з лишком на будь-який ненульовий елемент.

2. $R_1, R_2, \ldots, R_n$ - кільця. $a_i \in R_i, b_i \in R_i, c_i \in R_i, 1 \leq i \leq n$

   - **Асоціативність** $+$
     $(a_1, a_2, \ldots, a_n) + ((b_1, b_2, \ldots, b_n) + (c_1, c_2, \ldots, c_n)) = (a_1, a_2, \ldots, a_n) + (b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n) = (a_1 + b_1 + c_1, a_2 + b_2 + c_2, \ldots, a_n + b_n + c_n) = ((a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) + (c_1, c_2, \ldots, c_n)) = ((a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)) + (c_1, c_2, \ldots, c_n)$.
   - **Комутативність** $+$
     $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = (b_1 + a_1, b_2 + a_2, \ldots, b_n + a_n) = (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n)$.
   - **Наявність нуля**
     для будь-якого елементу $(a_1, a_2, \ldots, a_n)$ множини $R1 \times R2 \times \cdots \times Rn$ справедливо, що $(a_1, a_2, \ldots, a_n) + (0, 0, \ldots, 0) = (a_1, a_2, \ldots, a_n)$, де 0 - нульовий елемент $R1 \times R2 \times \cdots \times Rn$.
   - **Наявність одиничного елемента**
     Очевидно, що таким елементом є $(1, 1, \ldots, 1)$, де 1 - одиничний елемент кожного з кілець R1, R2, ..., Rn.
   - **Наявність протилежного елемента**
     для будь-якого елементу $(a_1, a_2, \ldots, a_n)$ множини $R1 \times R2 \times \cdots \times Rn$ існує протилежний елемент $(-a_1, -a_2, \ldots, -a_n)$ такий, що $(a_1, a_2, \ldots, a_n) + (-a_1, -a_2, \ldots, -a_n) = (0, 0, \ldots, 0)$.
   - **Асоціативність** $\cdot$
     $((a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n)) \cdot (c_1, c_2, \ldots, c_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n) \cdot (c_1, c_2, \ldots, c_n) = (a_1 b_1 c_1, a_2 b_2 c_2, \ldots, a_n b_n c_n) = (a_1, a_2, \ldots, a_n) \cdot (b_1 c_1, b_2 c_2, \ldots, b_n c_n) = (a_1, a_2, \ldots, a_n) \cdot ((b_1, b_2, \ldots, b_n) \cdot (c_1, c_2, \ldots, c_n))$.
   - **Дистрибутивність** $(a_1, a_2, \ldots, a_n) \cdot ((b_1, b_2, \ldots, b_n) + (c_1, c_2, \ldots, c_n)) = (a_1 \cdot (b_1 + c_1), a_2 \cdot (b_2 + c_2), \ldots, a_n \cdot (b_n + c_n)) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n) + (a_1 c_1, a_2 c_2, \ldots, a_n c_n) = (a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n) \cdot (c_1, c_2, \ldots, c_n)$
   - **Замкненість**
     $(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n) \in R1 \times R2 \times \cdots \times Rn$

3. Для того, щоб довести, що добуток полів $F_1 \times F_2 \times \ldots F_n$ з операціями покомпонентного додавання та множення не є полем, достатньо знайти контрприклад. Наприклад, якщо взяти поля $F_1 = \{0, 1\}, F_2 = \{0, 1\}$, то їх добуток $F_1 \times F_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ з операціями покомпонентного додавання та множення не є полем, оскільки $((1, 0)(0, 1) = (0, 0)$ і $(0, 1)(1, 0))$, тому не існує оберненого елемента для елементу (1,0) та (0,1)).

4. $f(x) = (2x^2 + 2x + 2) \cdot g(x) + (2x^5 + x^3 + x^2 + 2x)$,
   $g(x) = (x + 2)(2x^5 + x^3 + x^2 + 2x) + (2x^4 + 2x^3 + 2x + 2)$,
   $(2x^5 + x^3 + x^2 + 2x) = (x + 2)(2x^4 + 2x^3 + 2x + 2) + 2$
   $(2x^4 + 2x^3 + 2x + 2) = (x^4 + x^3 + x + 1) \cdot 2 + 0$
   $\gcd(f(x), g(x)) = 2$