Тема:
Деление многочленов в конечных полях

Сергей Витальевич Рыбин

svrybin@etu.ru

СПбГЭТУ «ЛЭТИ», кафедра «Алгоритмической математики»

21 января 2023 г.

Основные сведения

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:
$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

Основные сведения

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Основные сведения

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Основные сведения

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Арифметические действия в конечных полях

Сложение, вычитание и умножение в поле вычетов $\mathbb{Z}_p$ производим как для обычных целых чисел, просто выполняя действия в $\mathbb{Z}$ и беря результат из наименьшей положительной системы вычетов (добавляя или вычитая модуль p).

СПбГЭТУ «ЛЭТИ» ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Арифметические действия в конечных полях

Сложение, вычитание и умножение в поле вычетов $\mathbb{Z}_p$ производим как для обычных целых чисел, просто выполняя действия в $\mathbb{Z}$ и беря результат из наименьшей положительной системы вычетов (добавляя или вычитая модуль p).

Примеры

$$\begin{aligned} 1 - 2 = -1 &= 2 \pmod 3, \\ 3 + 5 = \ \ 8 &= 1 \pmod 7, \\ 3 \times 3 = \ \ 9 &= 4 \pmod 5. \end{aligned}$$

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Арифметические действия в конечных полях

Сложение, вычитание и умножение в поле вычетов $\mathbb{Z}_p$ производим как для обычных целых чисел, просто выполняя действия в $\mathbb{Z}$ и беря результат из наименьшей положительной системы вычетов (добавляя или вычитая модуль p).

Примеры

$$\begin{aligned} 1-2 = -1 &= 2 \pmod 3, \\ 3+5 = \quad 8 &= 1 \pmod 7, \\ 3\times 3 = \quad 9 &= 4 \pmod 5. \end{aligned}$$

Обратный элемент можно найти также, как и при решении сравнений $ax = 1 \pmod p$.

Основные сведения

1 Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2 Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Арифметические действия в конечных полях

Сложение, вычитание и умножение в поле вычетов $\mathbb{Z}_p$ производим как для обычных целых чисел, просто выполняя действия в $\mathbb{Z}$ и беря результат из наименьшей положительной системы вычетов (добавляя или вычитая модуль p).

Примеры

$$\begin{aligned} 1 - 2 = -1 &= 2 \pmod{3}, \\ 3 + 5 = \quad 8 &= 1 \pmod{7}, \\ 3 \times 3 = \quad 9 &= 4 \pmod{5}. \end{aligned}$$

Обратный элемент можно найти также, как и при решении сравнений $ax = 1 \pmod{p}$.

Для небольших p задачу можно решить простым перебором. Например, $3x = 1 \pmod{7}$. Перебирая возможные значения $x = 0, 1, 2, 3, 4, 5, 6$ получаем $x = 5, 3 \times 5 = 1 \pmod{7}$

Основные сведения

1. Для многочленов $A(x)$ и $B(x)$ с коэффициентами из поля K справедливо представление:

$$A(x) = B(x)Q(x) + R(x), \quad 0 \leqslant \deg R < \deg B. \tag{1}$$

Многочлен $Q(x)$ называют **частным** от деления $A(x)$ на $B(x)$, а $R(x)$ — соответственно **остатком**.

2. Представление (1) для многочленов над конечными полями играет важную роль в криптографии.

Далее в качестве конечных полей будем рассматривать поля вычетов $\mathbb{Z}_p$ для различных простых p.

Арифметические действия в конечных полях

Сложение, вычитание и умножение в поле вычетов $\mathbb{Z}_p$ производим как для обычных целых чисел, просто выполняя действия в $\mathbb{Z}$ и беря результат из наименьшей положительной системы вычетов (добавляя или вычитая модуль p).

Примеры

$$\begin{aligned} 1 - 2 = -1 &= 2 \pmod 3, \\ 3 + 5 = \quad 8 &= 1 \pmod 7, \\ 3 \times 3 = \quad 9 &= 4 \pmod 5. \end{aligned}$$

Обратный элемент можно найти также, как и при решении сравнений $ax = 1 \pmod p$.

Для небольших p задачу можно решить простым перебором. Например, $3x = 1 \pmod 7$. Перебирая возможные значения $x = 0, 1, 2, 3, 4, 5, 6$ получаем $x = 5, 3 \times 5 = 1 \pmod 7$

Представление (1) получаем обычным **делением столбиком**, с учетом сделанных замечаний о действиях в поле $\mathbb{Z}_p$.

Пример 1

Пример 1

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Покажем процесс деления подробно, по шагам.

Пример 1

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Покажем процесс деления подробно, по шагам.

1. Учитывая, что $2 \times 2 = 4 = 1 \pmod 3$, $-1 = -1 + 3 = 2 \pmod 3$, получаем:

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

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Покажем процесс деления подробно, по шагам.

1. Учитывая, что $2 \times 2 = 4 = 1 \pmod 3$, $-1 = -1 + 3 = 2 \pmod 3$, получаем:

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

2. Далее имеем:

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

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Покажем процесс деления подробно, по шагам.

1. Учитывая, что $2 \times 2 = 4 = 1 \pmod 3$, $-1 = -1 + 3 = 2 \pmod 3$, получаем:

$$\begin{array}{rrrrrr|l} x^5 & + & 2x^3 & + x^2 & & +2 & 2x^3+2x^2+x+2 \\ \cline{7-7} x^5 & + x^4 & + 2x^3 & + x^2 & & & 2x^2 \\ \cline{1-5} & 2x^4 & & & & +2 & \end{array}$$

2. Далее имеем:

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

3. Окончательно получаем:

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

СПбГЭТУ «ЛЭТИ» ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Задача

Найти представление (1) для многочленов

$$A(x) = x^5 + 2x^3 + x^2 + 2, \quad B(x) = 2x^3 + 2x^2 + x + 2$$

над полем $\mathbb{Z}_3$.

Покажем процесс деления подробно, по шагам.

1. Учитывая, что $2 \times 2 = 4 = 1 \pmod 3$, $-1 = -1 + 3 = 2 \pmod 3$, получаем:

$$\begin{array}{rrrrrr|l}
x^5 + & & 2x^3 & + x^2 & & +2 & 2x^3 + 2x^2 + x + 2 \\ \cline{7-7}
x^5 & + x^4 & + 2x^3 & + x^2 & & & 2x^2 \\ \cline{1-4}
& 2x^4 & & & & +2 &
\end{array}$$

2. Далее имеем:

$$\begin{array}{rrrrrr|l}
2x^4 & & & & & +2 & 2x^3 + 2x^2 + x + 2 \\ \cline{7-7}
2x^4 & + 2x^3 & + x^2 & + 2x & & & x \\ \cline{1-4}
& x^3 & + 2x^2 & + x & +2 & &
\end{array}$$

3. Окончательно получаем:

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

4. Получаем искомое представление

$$x^5 + 2x^3 + x^2 + 2 = \left(2x^3 + 2x^2 + x + 2\right)\left(2x^2 + x + 2\right) + x^2 + 2x + 1.$$

Пример 2

Пример 2

Задача

Найти представление (1) для многочленов

$$A(x) = 4x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 1, \quad B(x) = 3x^3 + 2x^2 + 3x + 1$$

над полем $\mathbb{Z}_5$.

Задача

Найти представление (1) для многочленов

$$A(x) = 4x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 1, \quad B(x) = 3x^3 + 2x^2 + 3x + 1$$

над полем $\mathbb{Z}_5$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_5$:

$$1 - 4 = -3 = 2 \pmod 5, \quad 1 - 2 = -1 = 4 \pmod 5, \quad 3 - 4 = -1 = 4 \pmod 5,$$
$$3 \times 3 = \ \ 9 = 4 \pmod 5, \quad 3 \times 2 = \ \ 6 = 1 \pmod 5.$$

Задача

Найти представление (1) для многочленов

$$A(x) = 4x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 1, \quad B(x) = 3x^3 + 2x^2 + 3x + 1$$

над полем $\mathbb{Z}_5$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_5$:

$$1 - 4 = -3 = 2 \pmod 5, \quad 1 - 2 = -1 = 4 \pmod 5, \quad 3 - 4 = -1 = 4 \pmod 5,$$
$$3 \times 3 = 9 = 4 \pmod 5, \quad 3 \times 2 = 6 = 1 \pmod 5.$$

2. Получаем:

$$\begin{array}{rrrrrr|l}
4x^5 & +2x^4 & +2x^3 & +3x^2 & +3x & +1 & 3x^3+2x^2+3x+1 \\ \cline{7-7}
4x^5 & +\ x^4 & +4x^3 & +3x^2 & & & 3x^2+2x+3 \\ \cline{1-4}
 & x^4 & +3x^3 & & +3x & +1 & \\
 & x^4 & +4x^3 & & +2x & & \\ \cline{2-6}
 & & 4x^3 & & +\ x & +1 & \\
 & & 4x^3 & +\ x^2 & +4x & +3 & \\ \cline{3-6}
 & & & 4x^2 & +2x & +3 &
\end{array}$$

Пример 2

Задача

Найти представление (1) для многочленов

$$A(x) = 4x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 1, \quad B(x) = 3x^3 + 2x^2 + 3x + 1$$

над полем $\mathbb{Z}_5$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_5$:

$$\begin{aligned} &1 - 4 = -3 = 2 \pmod 5, \quad 1 - 2 = -1 = 4 \pmod 5, \quad 3 - 4 = -1 = 4 \pmod 5, \\ &3 \times 3 = \ \ 9 = 4 \pmod 5, \quad 3 \times 2 = \ \ 6 = 1 \pmod 5. \end{aligned}$$

2. Получаем:

$$\begin{array}{rrrrrr|l} 4x^5 & +2x^4 & +2x^3 & +3x^2 & +3x & +1 & 3x^3 + 2x^2 + 3x + 1 \\ \cline{7-7} 4x^5 & + \ x^4 & +4x^3 & +3x^2 & & & 3x^2 + 2x + 3 \\ \cline{1-4} & x^4 & +3x^3 & & +3x & +1 & \\ & x^4 & +4x^3 & & +2x & & \\ \cline{2-6} & & 4x^3 & & + \ x & +1 & \\ & & 4x^3 & + \ x^2 & +4x & +3 & \\ \cline{3-6} & & & 4x^2 & +2x & +3 & \end{array}$$

3. Искомое представление:

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

Пример 3

Пример 3

Задача

Найти представление (1) для многочленов

$$A(x) = 6x^5 + 4x^4 + x^3 + 3x^2, \quad B(x) = 5x^3 + 3x^2 + 3x + 1$$

над полем $\mathbb{Z}_7$.

Пример 3

Задача

Найти представление (1) для многочленов

$$A(x) = 6x^5 + 4x^4 + x^3 + 3x^2, \quad B(x) = 5x^3 + 3x^2 + 3x + 1$$

над полем $\mathbb{Z}_7$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_7$:

$$3 - 5 = -2 = 5 \pmod 7, \quad -1 = 6 \pmod 7,$$

$$4 \times 5 = 20 = 6 \pmod 7, \quad 4 \times 3 = 12 = 5 \pmod 7.$$

Задача

Найти представление (1) для многочленов

$$A(x) = 6x^5 + 4x^4 + x^3 + 3x^2, \quad B(x) = 5x^3 + 3x^2 + 3x + 1$$

над полем $\mathbb{Z}_7$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_7$:

$$3 - 5 = -2 = 5 \pmod 7, \quad -1 = 6 \pmod 7,$$
$$4 \times 5 = 20 = 6 \pmod 7, \quad 4 \times 3 = 12 = 5 \pmod 7.$$

2. Получаем:

$$\begin{array}{rrrrrr|l}
6x^5 & +4x^4 & +\ x^3 & +3x^2 & & & 5x^3+3x^2+3x+1 \\ \cline{7-7}
6x^5 & +5x^4 & +5x^3 & +4x^2 & & & 4x^2+4x+1 \\ \cline{1-4}
 & 6x^4 & +3x^3 & +6x^2 & & & \\
 & 6x^4 & +5x^3 & +5x^2 & +4x & & \\ \cline{2-5}
 & & 5x^3 & +\ x^2 & +3x & & \\
 & & 5x^3 & +3x^2 & +3x & +1 & \\ \cline{3-6}
 & & & 5x^2 & & +6 &
\end{array}$$

Пример 3

Задача

Найти представление (1) для многочленов

$$A(x) = 6x^5 + 4x^4 + x^3 + 3x^2, \quad B(x) = 5x^3 + 3x^2 + 3x + 1$$

над полем $\mathbb{Z}_7$.

1. Аналогично предыдущему примеру используем равенства в $\mathbb{Z}_7$:

$$3 - 5 = -2 = 5 \pmod 7, \quad -1 = 6 \pmod 7,$$

$$4 \times 5 = 20 = 6 \pmod 7, \quad 4 \times 3 = 12 = 5 \pmod 7.$$

2. Получаем:

$$\begin{array}{rrrrrr|l}
6x^5 & +4x^4 & +x^3 & +3x^2 & & & 5x^3+3x^2+3x+1 \\ \cline{7-7}
6x^5 & +5x^4 & +5x^3 & +4x^2 & & & 4x^2+4x+1 \\ \cline{1-4}
 & 6x^4 & +3x^3 & +6x^2 & & & \\
 & 6x^4 & +5x^3 & +5x^2 & +4x & & \\ \cline{2-5}
 & & 5x^3 & +x^2 & +3x & & \\
 & & 5x^3 & +3x^2 & +3x & +1 & \\ \cline{3-6}
 & & & 5x^2 & & +6 &
\end{array}$$

3. Искомое представление:

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

Задачи для самостоятельного решения

Задача: Найти остаток от деления многочленов.

СПбГЭТУ «ЛЭТИ» ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Ответ: $3x^2 + x + 2$

Задачи для самостоятельного решения

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Ответ: $3x^2 + x + 2$

3. $x^5 + x^3 + 2^x + 2$ и $x^3 + x^2 + x + 1$ над полем $\mathbb{Z}_3$

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Ответ: $3x^2 + x + 2$

3. $x^5 + x^3 + 2^x + 2$ и $x^3 + x^2 + x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + 2x + 1$

Задачи для самостоятельного решения

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Ответ: $3x^2 + x + 2$

3. $x^5 + x^3 + 2^x + 2$ и $x^3 + x^2 + x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + 2x + 1$

4. $x^5 + 4x^3 + x^2 + x + 3$ и $x^3 + 4x^2 + 3x + 2$ над полем $\mathbb{Z}_5$

Задачи для самостоятельного решения

СПбГЭТУ «ЛЭТИ» ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Задача: Найти остаток от деления многочленов.

1. $2x^5 + x^4 + 2x^3 + x^2 + x$ и $x^3 + x^2 + 2x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + x + 1$

2. $6x^5 + 4x^4 + 4x^3 + 3x^2 + x + 4$ и $4x^3 + 3x^2 + 4x + 1$ над полем $\mathbb{Z}_7$

Ответ: $3x^2 + x + 2$

3. $x^5 + x^3 + 2^x + 2$ и $x^3 + x^2 + x + 1$ над полем $\mathbb{Z}_3$

Ответ: $2x^2 + 2x + 1$

4. $x^5 + 4x^3 + x^2 + x + 3$ и $x^3 + 4x^2 + 3x + 2$ над полем $\mathbb{Z}_5$

Ответ: $3x^2 + 3x + 4$

Литература

Литература

1. *С. В. Рыбин.* Дискретная математика и информатика. — Лань, 2022.

Литература

1. *С. В. Рыбин.* Дискретная математика и информатика. — Лань, 2022.
2. *С. Н. Поздняков, С. В. Рыбин.* Дискретная математика. — Издательский центр «Академия», 2008.