Некоторые группы обратимых многочленов с целыми коэффициентами по модулю многочлена и степени простого числа

К. Зюбин
Томск, МАОУ СОШ № 32, 11Б, 2022

Аннотация

В настоящей статье рассматриваются классы эквивалентности по модулю степени простого числа p^k и многочлена с целыми коэффициентами $P(x)$, старший коэффициент и свободный член которого не делятся на p. Описывается группа обратимых классов эквивалентности таких, что все элементы этих классов сравнимы с 1 по модулю p и $P(x)$.

1 Введение

В системе шифрования с открытым ключом MMMC1, предложенной С. К. Росошеком, для создания ключей шифрования используется мультипликативная группа факторкольца $\mathbb{Z}_{2^k}[x]/\langle x^2-1\rangle$, которая исследовалась в работе [1]. Естественно возникает вопрос об изучении мультипликативных групп факторколец $\mathbb{Z}_{p^k}[x]/\langle P(x)\rangle$ для произвольных многочленов $P(x)$ и простых p.

Будем говорить, что многочлены $A(x)$ и $B(x)$ с целыми коэффициентами сравнимы по модулю числа q и многочлена $P(x)$ с целыми коэффициентами, если существуют многочлены $U(x)$ и $V(x)$ с целыми коэффициентами такие, что

$$A(x) - B(x) = P(x)U(x) + qV(x).$$

Будем обозначать это как $A(x) \equiv B(x) \pmod{q, P}$. Формально, $A(x)$ и $B(x)$ сравнимы по модулю числа q и многочлена $P(x)$, если они принадлежат одному классу эквивалентности факторкольца $\mathbb{Z}[x]/\langle q, P\rangle$ кольца многочленов $\mathbb{Z}[x]$ по идеалу, порождённому числом q и многочленом $P(x)$.

Рассмотрим классы эквивалентности многочленов по модулю числа q и многочлена $P(x)$. Обозначим класс эквивалентности, содержащий многочлен $A(x)$ через $[A(x)]_{q,P}$. Над классами эквивалентности можно совершать операции сложения и умножения, аналогично сложению и умножению по модулю целого числа.

Будем говорить, что многочлен $A(x)$ с целыми коэффициентами обратим по модулю числа q и многочлена $P(x)$ с целыми коэффициентами, если существует многочлен $B(x)$ такой, что

$$A(x)B(x) \equiv 1 \pmod{q, P}.$$

Если один многочлен из класса эквивалентности обратим, то остальные многочлены этого класса тоже обратимы. Назовём класс эквивалентности, все элементы которого обратимы, обратимым классом эквивалентности.

Обозначим через $H_{p,k}(P(x))$ множество классов эквивалентности по модулю $q = p^k$, где p — простое, и $P(x)$ таких, что все элементы этих классов сравнимы с 1 по модулю p и $P(x)$. Множество $H_{p,k}(P(x))$ является группой относительно операции умножения классов эквивалентности по модулю p^k и $P(x)$. Заметим, что все элементы этой группы являются обратимыми классами эквивалентности.

Основным результатом работы является

Гипотеза. *Пусть $p > 2$ — простое, k — натуральное, $P(x)$ — многочлен с целыми коэффициентами, старший коэффициент которого не делится на p, $\deg P = n$. Тогда*

1) группа $H_{p,k}(P(x))$ изоморфна $(\mathbb{Z}_{p^{k-1}})^n$;

2) каждый элемент группы $H_{p,k}(P(x))$ единственным образом представляется в виде произведения элементов множества $\left\{ [1+px^s]_{p^k,P} \middle| 0 \leqslant s \leqslant n-1 \right\}$ в степенях меньших p^{k-1}.

Список литературы

[1] Зюбин К. С., *Описание строения группы обратимых центросимметричных двумерных матриц над $\mathbb{Z}_{2^k}$*, ММКШ, 2021, `https://www.mccme.ru/circles/oim/mmks/works2021/zyubin7.pdf`