исследования по увеличению класса примеров решения линейных дифференциальных уравнений с $\delta-$образными коэффициентами и свободными членами, а также влияния на решения постоянных слагаемых в коэффициентах, ассоциированных с нулем.

Литература:

1. Антоневич, А.Б. Об общем методе построения алгебр обобщенных функций / А.Б. Антоневич, Я.В. Радыно // Докл. АН СССР. – 1991. – Т.312, № 2. – С. 267-270.

2. Антоневич, А.Б. Линейные дифференциальные уравнения с обобщенными коэффициентами с точки зрения мнемофункций / А.Б. Антоневич, А.В. Турло // Дифференц. уравнения. – 1994. – Т.30, № 5. – С. 758-767.

УДК003.26:51:004(075.8)

Полиномиальные кольца классов вычетов в защите информации

Королева М.Н., Липницкий В.А.
Белорусский национальный технический университет

Пусть $\mathbb{Z}_p$ – кольцо классов вычетов по модулю простого числа, пусть $\mathbb{Z}_p[x]$ – кольцо полиномов с коэффициентами из $\mathbb{Z}_p$. Зафиксируем натуральное число $n>1$. В помехоустойчивом кодировании основополагающую роль играет фактор-кольцо $R_n=\mathbb{Z}_p[x]/<x^n-1>$ кольца $\mathbb{Z}_p[x]$ по идеалу $<x^n-1>$, порожденному полиномом x^n-1. Идеалы кольца R_n интерпретируются как циклические коды длиной n, определённые над полем Галуа $\mathbb{Z}_p$ (как правило, $p=2$). Как и в кольце $\mathbb{Z}_p[x]$, все идеалы кольца R_n являются главными: в каждом собственном идеале $J\subset R_n$ найдется полином $m(x)\neq 0$ наименьшей степени, тогда $J=<m(x)>-$ совпадает с главным идеалом, порожденным полиномом $m(x)$. Поскольку всякий собственный идеал любого кольца состоит из необратимых элементов этого кольца, полином $m(x)$ неизбежно обязан быть делителем полинома x^n-1.

В 1994 г. была создана криптосистемы NTRU именно на основе кольца R_n. Её циклические коды порождаются делителями x^n-1, принадлежащими классу круговых полиномов. NTRU использует в

качестве основных параметров полиномы обратимые в кольце R_n. Авторами исследованы необходимые признаки обратимости элементов кольца R_n, которые позволяют отсеивать заведомо негодные для построения конкретной криптосистемы NTRU полиномы. Публикации последних лет свидетельствуют о достаточной криптографической стойкости системы NTRU при $n>150$ и $p=3$. При таких значениях n алгоритмы Евклида, хотя и имеют полиномиальную сложность, требуют достаточно много времени для своей реализации. Для построения реальных криптосистем NTRU просто необходимы инструменты для отсеивания неудачных (необратимых) полиномов кольца R_n.

УДК 517.948.32:517.544

О проблеме обращения Якоби на римановой поверхности с краем

Крушевский Е.А.
Белорусский национальный технический университет

Рассмотрена классическая проблема обращения Якоби $\sum_{\nu=1}^{h}\zeta(q_\nu)\equiv q_\mu - k_\mu$ (mod периодов), где все обозначений была взята из [1], [2] для римановой поверхности рода $h\geq 1$ с краем. Реализация поверхности представлена как пространственная многосвязная область с m «дырками» и h «ручками». Каноническое рассечение (при помощи A-сечений и B-сечений) такой поверхности конформно эквивалентно $m+2h+1$-связной области с достаточно гладким краем, лежащей в верхней полуплоскости. При этом можно считать, что граничная кривая отображена на действительную полуось. Классические результаты гарантируют существование m линейно независимых над полем **R** абелевых дифференциалов 1-го рода $dw_1(z),...,dw_m(z)$, которые являются комплексно нормированными (матрица A-сечений является единичной, а матрица B-сечений – чисто мнимая с положительно определенной мнимой частью). С другой стороны при рассечении «ручек» возникает пара конформно склеенных «дырок», что при переходе к дублю римановой поверхности ведет к появлению дополнительных $2h$ линейно независимых над полем **R** абелевых дифференциалов 1-го рода $d\tilde{w}_{m+1}(z),...,d\tilde{w}_{m+2h}(z)$, которые не обладают свойством комплексной нормированности. Однако, используя принцип симметрии и метод ортогонализации, можно получить недостающие h базисных элементов по формуле $dw_{m+k}(z)=(d\tilde{w}_{m+k}(z)+\overline{d\tilde{w}_{m+2k}(\bar{z})})/2,\ k=\overline{1,h}$, обладающие свойством комплексной нормированности. Дальнейшая методика