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

решения проблемы обращения Якоби является стандартной для случая римановой поверхности рода 0.

Литература:

1. Чеботарев Н.Г. Теория алгебраических функций. – М.: Гостехиздат, 1948.
2. Зверович Э.И. Проблема обращения Якоби, ее аналоги и обобщения // Актуальные проблемы современного анализа. – Гродно, 2009. – С. 69-83.
3. Зверович Э.И., Задача о модуле аналитической функции для многосвязной области – Тезисы докладов XI Белорусской математической конференции, Минск, 2012. – ч. 1.

УДК 620.22:51-07

Решение задачи о проводимости волокнистых материалов с идеальными наполнителями и включениями

Кузнецова А.А.
Белорусский национальный технический университет

Задача о проводимости волокнистых материалов с наполнителями и включениями в статье [1] сведена к задаче Гильберта для некоторой специальной многосвязной области

$$\mathrm{Im}((t-a_k)\psi(t))=0, |t-a_k|=r_k, k=1,\ldots,n,$$

где известные константы a_k, r_k являются геометрическими характеристиками круговых наполнителей и включений, которая полностью решена в общем случае в [2; 3].

В настоящей работе был использован известный способ для исследования проводимости волокнистых материалов с двумя наполнители и/или включениями, которые являются идеальными кругами. Конкретизация структуры материала, несмотря на точные формулы [2] и [3], их сложная структура требует компьютерной реализации, что позволяет получить конструктивные формулы решения задачи Гильберта для комплексного потенциала. Решение получено в виде $\varphi_k(z)=\varphi_k^{(0)}(z)+\sum_{m=1}^{n}\beta_m\varphi_k^{(m)}(z)$, где для всех слагаемых построены явные аналитические выражения в виде равномерно сходящихся функциональных рядов и аппроксимирующих бесконечных произведений с использованием дробно-линейных отображений и мёбиусовых трансформаций. Также некоторые интересные практические результаты были вычислены на компьютере.

Литература:

1. Mityushev, V., Pesetskaya, E., Rogosin, S.: Analytical Methods for Heat