



Faculty of  
Science and  
Technology  
Tokushima University

# 整数論と代数系の応用

[キーワード: 代数体, 類数, 楕円曲線, 暗号]

教授 高橋浩樹

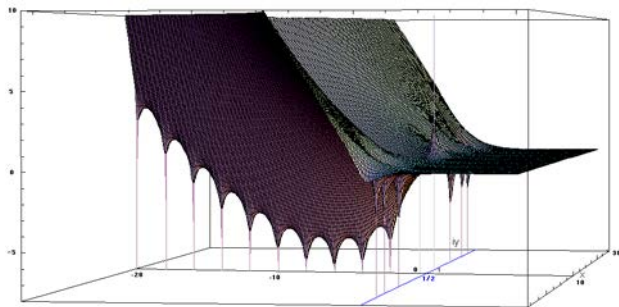


Fig.1  $\log|\zeta(s)|$  ( $\zeta(s)$ : リーマンゼータ関数)

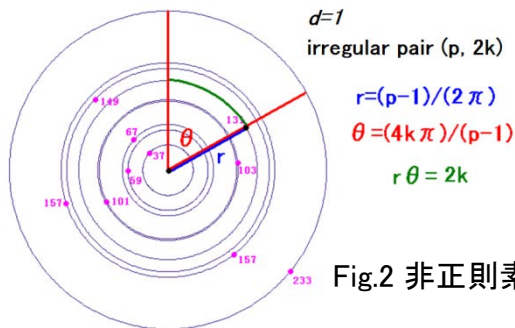


Fig.2 非正則素数および指数

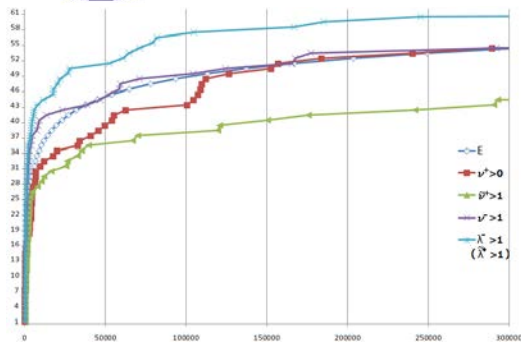


Fig.3 例外的な素数の個数

内容:

代数体のイデアル類群についての研究を進めている。特に実円分体の類数に関する二つの予想, Greenberg予想およびVandiver予想について, 計算機を用いながら調査している。さらに, 研究対象の代数体や楕円曲線といった代数系は暗号理論とも密接な関係があり, これらの新たな応用についても考察している。

リーマンゼータ関数は多くの数学者に興味を持たれている関数である(cf. Fig.1). その特殊値は円分体のイデアル類群と深い関係がある(cf. Fig.2). この深い関係は, 実円分体の類数と単数群と円単数群の指数の一致として表現できる。

Greenberg予想は, その差が無限次 $Z_p$ 拡大においても  $p$ 部分に関しては有界であろうという予想である。さらに, Vandiver予想は,  $p$ 円分体に限れば $p$ 部分は自明であろうという予想である。

これまで, 円単数, ガウス和,  $p$ 進 $L$ 関数といった数論的特殊元と補助的な素数たちを用いて, これらの予想に取り組んできた。その結果, Greenberg予想が成立する実例や岩澤不変量が例外的な値となる素数たちを計算機を用いて数多く発見することが可能となった(cf. Fig.3)。

分野: 数学

専門: 代数学

E-mail: hirokit@tokushima-u.ac.jp

Tel. 088-656-7549

Fax: 088-656-7549

HP : <http://hiro2.pm.tokushima-u.ac.jp/>

