論文審査の結果の要旨

氏名　坂川　日出海

E を有理数体 $\mathbf{Q}$ 上の楕円曲線とし, E のよい還元を与える素数 p に対し $E \bmod p$ の $\mathbf{F}_p$-有理点のなす有限群 $E_p(\mathbf{F}_p)$ を考える. $E_p(\mathbf{F}_p)$ が巡回群となるような素数 $p \leq x$ の個数を $f(x, E)$ と書く時, J. -P. Serre は一般 Riemann 予想 (GRH) を仮定して $f(x, E)$ の漸近挙動に関する評価式を与えた. 1979 年には R. Murty は E が虚数乗法を持てば, GRH の条件を落とせることを示した. 本論文において, 坂川日出海は, このような結果を踏まえ, まず, $E_p(\mathbf{F}_p)$ の位数が平方因子を持つような巡回群になる素数 $p \leq x$ の個数を $g(x, E)$ であらわすとき, $g(x, E)$ の漸近挙動を調べ次の結果を得た.

定理. E を虚数乗法をもたない楕円曲線, 素数 q に対し $E[q]$ を代数平方 $\bar{\mathbf{Q}}$ 上の q-torsion のなす群とする. ガロア群 $Gal(\mathbf{Q}(E[q])/\mathbf{Q}) \cong GL_2(\mathbf{F}_q)$ が成り立つと仮定する. このとき., GRH の下に E のみによる定数 C_E が存在して

$$g(x, E) \geq C_E x / \log x$$

が成り立つ.

次に, 正の定数 α に対し, $E_p(\mathbf{F}_p)$ の位数が x^α 以下の素数で割り切れないような素数 $p \leq x$ の数の計数関数 $\pi^\alpha(x, E)$ を導入し, 次の結果を得た.

定理. E を虚数乗法をもたない楕円曲線で非自明なねじれを持たないとする. このとき, GRH の下に, E のみによる定数 A_E, B_E が存在して,

$$A_E x / \log x \leq \pi^{1/21}(x, E) \leq B_E x / \log x$$

が成り立つ.

この結果は A. Artin と R. Murty の手法に基づくものであるが, 計数関数 $\pi^\alpha(x, E)$ を導入することにより評価を厳しいものにしている. さらに, Koblitz 予想を拡張して, k を任意の自然数とするとき, $E_p(\mathbf{F}_p)$ の位数が丁度 k 個の相異なる素数の積で表されるような素数 $p \leq x$ の個数が $C_{E,k} x (\log\log x)^{k-1} / (\log x)^2$ で近似されるという予想をたて, 計算機実験によってそれを裏付けるデータを与えている.

本論文は, 有理数体 $\mathbf{Q}$ 上の楕円曲線という古典的な対象を扱い, そのよい還元を与える素数 p に対して $\mathbf{F}_p$ 上の楕円曲線の有理点が巡回群になる

ようなものの分布に関する新しい知見を与え, 興味あるデータを示したもので, この方面の研究に大きく貢献するものである. よって、論文提出者
坂川　日出海は、博士（数理科学）の学位を受けるにふさわしい充分な資格があると認める。