論文の内容の要旨

論文題目　Study of Group orders of Elliptic curves
(楕円曲線の群位数の研究)

氏名　坂川　日出海

1　巡回性

E を、有理数体 $\mathbb{Q}$ 上定義された楕円曲線とする。E の良い素数（good prime）p に対し、$E_p(\mathbb{F}_p)$ で $E \mod p$ 上の $\mathbb{F}_p$-有理点のなす有限群を表す。我々は、p が動くときの、$E_p(\mathbb{F}_p)$ の漸近的な挙動に興味がある。まず始めに巡回性の問題について考察する。$f(x, E)$ で、$E_p(\mathbb{F}_p)$ が巡回群となるような素数 $p \leq x$ の個数を表そう。この計数関数（counting function）の漸近的な挙動に関して、1976 年に、J.P.Serre[5] は次の結果を得た。

定理 1. 一般 Riemann 予想（以下 GRH と記す）のもとで、E のみに依る実数 C_E が存在して、次の評価がなりたつ；

$$f(x, E) = C_E \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right).$$

その後、1979 年に、Ram Murty[3] により、E が虚数乗法を持つ場合には、上の定理が無条件で成り立つことが示された。一般の場合は現在でも未解決である。

ところで、有限 Abel 群の基本定理より、$\sharp E_p(\mathbb{F}_p)$ が平方自由（square-free）であれば、それは明らかに巡回群である。ここに次の自然な疑問が生じる。すなわち、群位数が平方因子を持ち、なおかつ巡回群となるような、素数 $p \leq x$ の個数は、どのような漸近挙動を示すのであろうか？先の $f(x, E)$ に習い、今の場合の計数関数を $g(x, E)$ で表す。この関数の漸近挙動に関して、筆者は次の結果を得た。

主結果 1. E を虚数乗法を持たない楕円曲線で、すべての素数 q に対して、同型 $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \cong \mathrm{GL}_2(q)$ が成り立つものとする。この時、GRH の仮定のもとで、

E のみに依る正の実数 C_E が存在して、次の評価が成り立つ。特にそのような素数の集合は、正の密度を持つ；

$$g(x,E) \geq C_E \frac{x}{\log x}.$$

2 素数性

巡回性に準ずる自然な問題は、$E_p(\mathbb{F}_p)$ が素数位数を持つような、素数 $p \leq x$ の個数を考察することである。素数位数の群は当然、巡回群だからである。この場合の計数関数を $\pi(x,E)$ で表そう。この関数の漸近挙動に関して、1988 年に N.Koblitz[2] は次の予想を立てた。

予想 1. E を $\mathbb{Q}$ 上定義された、非自明な捩れ点を持たない楕円曲線とする。この時、E のみによる正の実数 C_E が存在して、次の評価が成り立つ；

$$\pi(x,E) \sim C_E \frac{x}{(\log x)^2}.$$

その後、2001 年に、A.Miri と K.Murty[4] により次の結果が得られた。

定理 2. E を $\mathbb{Q}$ 上定義された、虚数乗法を持たない楕円曲線とする。また GRH を仮定せよ。この時、$\sharp E_p(\mathbb{F}_p)$ が重複を込めて高々 16 個の素因子を持つような、素数 $p \leq x$ の個数に関して、次が成り立つ；

$$\gg \frac{x}{(\log x)^2}.$$

しかしその後も、上限に関する結果は得られていない。上限について考察するために、筆者は計算機を用いて、前掲の Koblitz の予想の解析を試みた。その時に得られた数値データを、博士論文の末尾に収録した。筆者は計算結果により、Koblitz の予想を次のように拡張した。

予想. E を非自明な捩れ元を持たない、$\mathbb{Q}$ 上定義された楕円曲線とする。k を任意の自然数とする。この時、E と k のみに依る正の実数 $C_{E,k}$ が存在して、$\sharp E_p(\mathbb{F}_p)$ が丁度 k 個の相異なる素数の積で表されるような、素数 $p \leq x$ の個数に関して、次が成り立つ；

$$\sim C_{E,k} \frac{x(\log\log x)^{k-1}}{(\log x)^2}.$$

この予想を認めると、A.Miri と K.Murty が考察した計数関数の緊密な下限は、以下のオーダーを持つことになる；

$$\frac{x(\log\log x)^{15}}{(\log x)^2}.$$

上限と下限のオーダーが一致した結果を得るために筆者は、正の実数 α に対し、$\sharp E_p(\mathbb{F}_p)$ が x^α 以下の素数で割り切れないような、素数 $p \le x$ の計数関数 $\pi^\alpha(x,E)$ を考察した。良く知られた群位数に関する Hasse-Weil の定理より、

$$\pi(x,E) \sim \pi^{\frac{1}{2}}(x,E)$$

が分かる。計数関数 $\pi^{\frac{1}{22}}(x,E)$ に関して、筆者は次の結果を得た。

主結果 2. E を $\mathbb{Q}$ 上定義された、非自明な捩れ点を持たない楕円曲線で、虚数乗法を持たないものとする。この時、GRH のもとで、次を満たす E のみに依る実数 A_E、B_E が存在する；

$$A_E\frac{x}{(\log x)^2} \le \pi^{\frac{1}{22}}(x,E) \le B_E\frac{x}{(\log x)^2}.$$

最後に、GRH の仮定を外した、次の結果を得た。証明は C.Cojocaru が [1] で用いた論法に依るところが大きい。

主結果 3. E を $\mathbb{Q}$ 上定義された楕円曲線で、虚数乗法を持たないものとする。この時、無条件に次がなりたつ；

$$\pi(x,E) = O\left(\frac{x}{\log x}\frac{1}{\log\log\log x}\right).$$

特に、$\sharp E_p(\mathbb{F}_p)$ が素数となるような素数 p の密度はゼロである；

$$\lim_{x\to\infty}\frac{\pi(x,E)}{\mathrm{Li}(x)} = 0.$$

参考文献

[1] Cojocaru, Alina Carmen. On the cyclicity of the group of $\mathbb{F}_p$ -rational points of non-CM elliptic curves. J. Number Theory 96 (2002), no. 2, 335–350.

[2] Koblitz, Neal. Primality of the number of points on an elliptic curve over a finite field. Pacific J. Math. 131 (1988), no. 1, 157–165.

[3] Murty, M. Ram. On Artin's conjecture. J. Number Theory 16 (1983), no. 2, 147–168.

[4] Miri, S. Ali; Murty, V. Kumar. An application of sieve methods to elliptic curves. Progress in cryptology—INDOCRYPT 2001 (Chennai), 91–98, Lecture Notes in Comput. Sci., 2247, Springer, Berlin, 2001.

[5] Serre, Jean-Pierre. Résumé des cours de 1977-1978, Annuaire du Collège de France. 1978, p. 67-70, in Collected Papers, volume III, Springer Verlag, 1986, p. 465-468.