数理解析研究所講究録
第721巻 1990年 176-183

Singular moduli と $\mathbb{Q}$ 上の楕円曲線の supersingular prime

阪大理 金子 昌信 (Masanobu Kaneko)

1989年1月の大阪大における整数論シンポジウムで, N. Elkies による $\mathbb{Q}$ 上の楕円曲線の supersingular prime の無限性の証明を紹介した。その報告集[10]の最後に Remark として述べた結果を再び Elkies が, supersingular prime の個数の上からの評価に応用した。講演では主にその応用を, [10]で紹介した手法を復習しつつ話した。以下では[10]と重複する部分は[10]を見ていただくことにして, 新しい箇所の筋道だけを記すことにする。(詳細は[5]及び[7]を参照して下さい。)

$E/\mathbb{Q}$ を有理数体上定義された, 虚数乗法をもたない楕円曲線とする。正の実数 x に対し $N_E(x)$ で E の x 以下の supersingular reduction prime の個数を表すことにする;

$$N_E(x) = \{p \mid p: \text{prime} \leq x,\ E \bmod p \text{ は supersingular}\}.$$

この時，1976年に S. Lang と H. Trotter [8] によって提出された予想に

$$N_E(x) \overset{?}{\underset{x\to\infty}{\sim}} c_E \frac{\sqrt{x}}{\log x} \quad (c_E \text{ は } E \text{ のみによるある正の定数})$$

というのがある*)が，未だ証明も否定もされていない．実際，$N_E(x)$ が ∞ に発散する（つまり supersingular prime が無限個ある）ことがようやく1987年に Elkies によって証明されたばかりで，その証明を effective にすることは出来るのだが GRH（一般リーマン予想）を使ってすら

$$N_E(x) \gg \log\log\log x$$

くらいのことがいえるにすぎない。(M. L. Brown [1])

一方 $N_E(x)$ を上から評価するのはどうかというと J. P. Serre [9] が1981年に，

$$N_E(x) = O\left(\frac{x}{(\log x)^{3/2-\delta}}\right) \quad (\forall \delta > 0)$$

---

*) 素朴に考えると …… a_p を Frobenius のトレースとすると Riemann 予想の類似によって $|a_p| < 2\sqrt{p}$. a_p が各値をとる確率が等しいなら（佐藤-Tate 予想によれば実際は違うはず）$a_p = 0$ (supersingular) の確率 $1/4\sqrt{p}$. これを"素数分布測度" $d\pi(x) \sim \frac{dx}{\log x}$ で積分して $\int^x \frac{1}{4\sqrt{x}} \cdot \frac{dx}{\log x} \sim \frac{1}{2}\frac{\sqrt{x}}{\log x}$ という $\frac{\sqrt{x}}{\log x}$ が出てくる。

及び，GRHの下で

$$N_E(x) = O(x^{3/4})$$

を示している．このGRHという仮定がはずせるというのが今度のElkiesの主張である．

Theorem (Elkies)
無条件に $N_E(x) = O(x^{3/4})$．
右辺に含まれる定数はEのみによるeffective constant.

証明のポイントは3つあって，Elkiesの書き方([4])に倣うと（記号は後で説明する）

1. pでsupersingular reductionのときE mod pは$|d| \ll p^{1/2}$なるある$\mathcal{O}_d$による虚数乗法をもつ．
2. そのときpは$P_d(j_E)$の分子を割る．
3. $P_d(j_E)$の分子を$|d| \le M$なるdについてかけたものの絶対値は$\exp(\text{const}\cdot M^{3/2}\log M)$のorderでおさえられる．

となる．ここに$\mathcal{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$は判別式dの虚2次order，$j_E$はEのj-不変量($\in\mathbb{Q}$)，$P_d(X)$は$\mathcal{O}_d$にCMをもつ楕円曲線/$\mathbb{Q}$のj-不変量の$\mathbb{Q}$上の最小多項式で[10]では
（これをsingular modulusという）

P_d と書いたもの。

x 以下の supersingular prime は 1. と 2. より $|d| \leq x$ なる $P_d(j_E)$ の分子に現れているのであるからその分子の大きさが評価できると $N_E(x)$ の上からの評価が得られるのである。(non-CM の仮定は $P_d(j_E) \neq 0$ を保証する。$=0$ だとやっていることに意味がなくなる)

3つのポイントのうち，1. が私のやった部分([7])。

2. は Elkies の $N_E(x) \to \infty$ の証の出発点となっている observation (の逆) で [10] で説明した。

3. の評価が新たに Elkies の行った部分で，$P_d(X)$ の次数は $\mathcal{O}_d$ の類数であるから $|d| \leq M$ なる $\mathcal{O}_d$ の類数の和を評価して j 関数の値の評価

$$\log |j(z)| = 2\pi \mathrm{Im}(z) + O(1)$$

と組み合わせることにより得られる([4])。

以下では 1. の部分をどのように示すかを簡単に述べる。

1. で言っていることは $E \bmod p$ の準同型環が $\mathcal{O}_d$ を含むということなのだが，楕円曲線の準同型環については古くから Deuring の仕事 [2] によってわかっていて，この場合 supersingular であるから，p と ∞ でのみ分岐する $\mathbb{Q}$ 上の四元

数環 $Q_{\infty,p}$ の極大整環になる。そこで問題は $Q_{\infty,p}$ の極大整環の中になるべく $|d|$ の小さな O_d をみつけるということになる。簡単のため $\sqrt{d}$ をみつける問題だとする。この元はつまりトレースが0，ノルムが $-d$ の元ということで，結局，極大整環の中のトレース=0で定まる rank 3 の lattice の元でノルムがなるべく小さいものをさがすことになる。この時，$|d| \ll p^{2/3}$ なるものが存在することが"geometry of numbers"の議論でわかり，[3]でも証明されている。

ところで，3.の評価でわかることは，$|d| \ll p^{\theta}$ なる評価から $N_E(x) = O(x^{\frac{3}{2}\theta})$ が出る，ということなので上のように $\theta = \frac{2}{3}$ では trivial な評価しか出てこない。

さて，今Eは $\mathbb{Q}$ 上定義されるとしているから E mod p は $\mathbb{F}_p$ 上定義される。この時 E mod p の準同型環は $Q_{\infty,p}$ の極大整環であって $\sqrt{-p}$ を含むものになる。(逆もいえて，きれいな対応がついている。) $\sqrt{-p}$ はすなわち p乗 Frobenius に対応する元である。このような極大整環は伊吹山さん[6]によって具体的に記述されている。それを用いて，トレース=0の他に，p乗 Frobenius と直交するという条件を加えた rank 2 の lattice を見てやる(何故こうするとうまくいくのか？)ことにより $|d| \ll p^{1/2}$ なるものの存在が言える。

計算によると，$|d| \ll p^{1/2}$ がとれるのは $\sqrt{-p}$ を含む整環に特(いつも)

有の現象であって，又 $\frac{1}{2}$ という exponent は best possible であると思われる。

なお，$|d| \ll p^{1/2}$ と書いたが，explicit な形は $|d| \leq \frac{4}{\sqrt{3}} p^{1/2}$ である。

References

[1] M.L. Brown, Note on supersingular primes of elliptic curves over $\mathbb{Q}$, Bull. London Math. 20 (1988)

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionen Körper, Abh. Math. Sem. Univ. Hamburg 14 (1941), 197-272

[3] N.D. Elkies, The Existense of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, Invent. Math. 89 (1987), 561-567

[4] ———, Letter to Serre, April 17, 1989

[5] ———, Journées Arithmétique (1989) 報告集, to appear in Astérisque.

[6] T. Ibukiyama, On maximal orders of division quaternion algebra over the rational number field with certain optimal embeddings, Nagoya Math. J. 88 (1982), 181-195.

[7] M. Kaneko, Supersingular j-invariants as singular moduli mod p,

[8] S. Lang - H. Trotter, Frobenius distributions in GL_2-extensions, Springer LNM 504 (1976).

[9] J.P. Serre, Quelques applications du théorème de densité

de Chebotarev, Publ. Math. IHES, n°54 (1981), 123-201
全集 vol. III, 563-641
[10] 整数論シンポジウム報告集 1989年 於 大阪大学