

楕円曲線の $Q(T)$ -rank に関する予想

滋賀職業能力開発短期大学校

長尾 孝一

On a Conjecture of $Q(T)$ -rank of Elliptic Curve

Kōichi NAGAO

要約 有理数体 Q や有理関数体 $Q(T)$ 上定義された楕円曲線の有理点や $Q(T)$ 有理点の作る群については、Mordell Weil の定理によって、それらが有限生成アーベル群となることが知られている。以下、これらの群の free-rank を簡単に rank と言う事にする。 Q 上定義された楕円曲線の rank に関しては有名な Birch, Swinnerton-Dyer 予想がある。ここでは、この予想をいじることによって、有理関数体 $Q(T)$ 上定義された楕円曲線の rank に関してその近似を与えることのできる予想を作る。又、特殊な場合において予想が正しく、又、計算機による数値実験を仮定すると予想が正しい場合があることをしめす。そして最後に、この予想と有名な Tate の予想との関係を述べる。

§ 1. 序、結果

記号 Q 上定義された楕円曲線 E に対して

$$\begin{aligned} a_p &= a_p(E) = p + 1 - \#E(F_p), \quad \alpha_p, \bar{\alpha}_p \text{ を} \\ (1 - \alpha_p T)(1 - \bar{\alpha}_p T) &= 1 - a_p T + pT^2, \\ b(p, m) &= \alpha_p^m + \bar{\alpha}_p^m \quad (m \in \mathbb{N}), \\ L_E(s) &= \prod_{p: \text{素数}} (1 - a_p p^{-s} + p^{1-2s}), \end{aligned}$$

とおく。

また、 $Q(T)$ 上定義された楕円曲線 E に対して、変数 T を有理数 t によって特殊化して得られる Q 上定義された楕円曲線を E_t とする。

また、 $A_p = A_p(\mathcal{E}) = \sum_{t=0}^{p-1} a_p(E_t) / p$ とおく。

この論文では、次の予想について考察する。

予想 「 $Q(T)$ 上定義された曲線 \mathcal{E} が Q 上では定義されていない時、

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数}, p \leq N} -A_p \cdot \log(p) \text{ は } \mathcal{E} \text{ の } Q(T)\text{-rank に}$$

収束する。」○

この予想が出来た経緯としてまず、 Q 上定義された楕円曲線に関する Birch, Swinnerton-Dyer 予想について述べる。

Birch, Swinnerton-Dyer 予想 「楕円曲線

E 、に対して、その L 関数 $L(s)$ は有理型関数として複素平面全体に解析接続でき、その $s=1$ での零点の位数が E の rank となる。」○

このとき、 $L(s)$ の対数微分 $L'(s)/L(s)$ を考える。

こうすると、rank は $s=1$ での留数 $\text{res}_{s=1} L'(s)/L(s)$ と書けるので扱いやすい。

実際、 $f_m = \sum_{p: \text{素数}} -\log(p) \cdot b(p, m) \cdot p^{-ms}$ とおくと、 $L'(s)/L(s) = \sum_{m=1}^{\infty} f_m(s)$ とかけ、次のことがわかる。

1. $\sum_{m \geq 3} f_m(s)$ は $\Re s \geq 1$ で収束する。

($|b(p, m)| \leq 2p^{m/2}$ より、わかる。)

2. 佐藤予想を仮定すると、

$\lim_{s \rightarrow 1+0} (s-1) \cdot f_2(s) = 1/2$ がわかる。

(§ 3 で示す。)

よって、 E の rank は $\text{rank} = 0.5 + \text{res}_{s=1} f_1(s)$ となることが、予想できる。

以下、 $Q(T)$ 上定義された楕円曲線 \mathcal{E} に対して我々の予想を導くため ad-hoc な議論を試みる。まず、 Q 上定義された楕円曲線の族 $\{E_t \mid t \in \mathbb{Z}\}$ に含まれる曲線の rank の平均を考察する。 $f_1(s) = \sum -a_p \cdot \log(p) \cdot p^{-s}$ に注意するとそれぞれの曲線に対して、

$rank$ of $(E_t) = 0.5 + res_{s=1} \{ \sum -a_p(E_t) \cdot \log(p) \cdot p^{-s} \}$ と書けるためこの族に含まれる曲線の $rank$ の平均は $0.5 + res_{s=1} \sum \{ -\{a_p(E_t) \text{の平均}\} \cdot \log(p) \cdot p^{-s} \}$ と書かれると予想される。また、 $t = s \pmod p$ の時 $a_p(E_t) \equiv a_p(E_s)$ に注意すると、これは $0.5 + res_{s=1} \sum \{ -A_p(\delta) \cdot \log(p) \cdot p^{-s} \}$ と書けると予想される。

命題 1-1 (Abel)

「ディリクレ級数 $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ (a_n は実数) が $\Re(s) > 1$ で収束し $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} a_n$ が収束する時

$$\lim_{s \rightarrow 1+0} (s-1) \cdot f(s) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} a_n$$

が成り立つ。」○

実験的に具体的な例において

$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} -A_p \cdot \log(p)$ は収束する。よって、上の族に含まれる曲線の $rank$ の平均は $0.5 + \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} -A_p \cdot \log(p)$ とかけると予想され、この値が δ の $Q(T)$ -rank と関係があると思えることより我々は上の予想を得た。

この予想に関して筆者は次のような結果を得た。

$f(X) \in Z(X)$ を重根を持たない monic な三次式とする。

定理 1 「 $Q(T)$ 上定義された楕円曲線 $Y^2 = f(X) + T$, ($Q(T)$ -rank = 0) に関して予想は成立する。」○

(この時、「 $A_p = 0$ 」が 任意の素数 p で成り立つことが簡単にわかる。)

定理 2 「 $Q(T)$ 上定義された楕円曲線 $Y^2 = f(X) + T^2$, ($Q(T)$ -rank は $F(X)$ が既約、二次式×一次式に分解、一次式×一次式×一次式に分解の時それぞれ 0, 1, 2 となる) に関して予想は成立する。」○

$$\delta_{E6}: Y^2 = X^3 + (-381 \cdot T^2 + 202752 \cdot T - 36577584) X + T^4 + 427420 \cdot T^2 - 319993344 \cdot T + 61357067136.$$

$$\delta_{E7}: Y^2 + 3^8 \cdot (T^3 - 2716410100150129 / 27 \cdot T - 281715490868677435751762 / (3^6)) X + 3^{12} \cdot (8878 / 3 \cdot T^4 + 1195761874250 / 27 \cdot T^3 + 1666490318377404686 / 9 \cdot T^2 + 20193960549267845801903566 / (3^7) \cdot T - 17219105683784186196665593491513616 / (3^9)).$$

$$\delta_{E8}: Y^2 = X^3 + 3^4 \cdot (-310 \cdot T^3 + 243896065 \cdot -60857017136860 \cdot T + 13936180986780637484 / 3) X + 3^6 \cdot (T^5 - 2763436738910 / 3 \cdot T^3 + 1681300207452917540 / 3 \cdot T^2$$

$$- 384550638908428401057560 / 3 \cdot T + 282412962406880649939736350128 / 27).$$

とする。これは、塩田 [1] によって作られた、 $Q(T)$ -rank がそれぞれ 6, 7, 8 の例である。(これらの例では $Q(T)$ -rank = $\overline{Q}(T)$ -rank である。)

上の三つの例で計算機による実験をすることにより、つぎの観察を得る。

観察 1 「十分大きな素数 p に対して $Q(T)$ -rank = $-A_p$ が成立しているように思われる。」○

定理 3 「この観察を仮定すると上の予想が δ_{E6} , δ_{E7} , δ_{E8} について成立する。」○

$$\delta_{k3}: Y^2 = X^3 - 3T^4 X - T^2(1 + T^8), \text{ とおく。}$$

($Q(T)$ -rank = 1 が桑田 [2] によって知られている。) ついての実験よりつぎの観察を得る。

観察 2 「この曲線について

$$A_p = \begin{cases} 2 & p \equiv 3 \pmod 4, p \neq 3 \text{ の時} \\ -4b^2/p & p \equiv 5 \pmod 8 \text{ の時} \\ (-4b^2 - 4p)/p & p \equiv 1 \pmod 8 \text{ の時} \end{cases}$$

が成り立つと思われる。

ただし、 b は $p = a^2 + b^2$ (a 偶数, b 奇数) を満たす唯一の自然数とする。」○

定理 4 「これを仮定すると上の予想は δ_{k3} に関して成立する。」○

§ 2 素数の密度

ここでは、定理の証明の為に素数の密度に関する結果を準備する。

記号 $\pi(N)$ を自然数 N 以下の素数の個数とおく。また、素数の部分集合 M と自然数 N に対して、

$$M(N) = \{ p \in M \mid p \leq N \} \text{ とおく。また、}$$

$$d(M) = \lim_{N \rightarrow \infty} \frac{1}{\pi(N)} \sum_{p \in M(N)} 1$$

$$\sigma(M) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p \in M(N)} \log(p)$$

とおく。

命題 2-1 「 $d(M)$, $\sigma(M)$ のうち一方が収束するとき他方も収束し、その値は等しい。」○

ここでは、もっと一般につきを示す。

補題 「素数を index にもつ非負、有界な数列 $\{c_p\}$ に対して、

$$\lim_{N \rightarrow \infty} \frac{1}{\pi(N)} \sum_{p: \text{素数} \leq N} c_p, \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} \log(p) \cdot c_p$$

はその一方が収束するとき他方も収束し、その値は等しい。」 \odot

証明 $|c_p| < K$ とする。また、

$$\vartheta(N) = \sum_{p: \text{素数} \leq N} \log(p) \cdot c_p, V(N) = \sum_{p: \text{素数} \leq N} c_p, \text{ とおく。}$$

ここで、 $\vartheta(N) < \log(N) \cdot V(N)$ がわかる。

また、 $0 < \delta < 1$ を満たす任意の δ に対して

$$\begin{aligned} \vartheta(N) &\geq \sum_{N^\delta < p < N} \log(p) \cdot c_p \\ &\geq \delta \cdot \log(N) \cdot \sum_{N^\delta < p < N} c_p \\ &= \delta \cdot \log(N) \cdot \sum_{p < N} c_p - \delta \cdot \log(N) \cdot \sum_{p < N^\delta} c_p \\ &\geq \delta \cdot \log(N) \cdot \sum_{p < N} c_p - K \cdot N^\delta \cdot \log(N) \\ &= \delta \cdot \log(N) \cdot V(N) - K \cdot N^\delta \cdot \log(N) \text{ がわかる。} \end{aligned}$$

よって、素数定理 ($\pi(N) \sim N/\log(N)$) より、

$$\begin{aligned} \limsup_{N \rightarrow \infty} \vartheta(N)/N &\leq \liminf_{N \rightarrow \infty} V(N) \cdot \log(N)/N \\ &= \liminf_{N \rightarrow \infty} V(N)/\pi(N) \end{aligned}$$

$$\begin{aligned} \liminf_{N \rightarrow \infty} \vartheta(N)/N &\leq \limsup_{N \rightarrow \infty} \delta \cdot V(N) \cdot \log(N)/N \\ &= \limsup_{N \rightarrow \infty} \delta \cdot V(N)/\pi(N) \end{aligned}$$

がわかる。q.e.d.

上の命題より次を得る。

系 2-1 $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} \log(p) = 1 \quad \odot$

この系より我々は簡単に定理 1、定理 3 の証明を得る。

一方、有限次代数体 K に対して、

$$c_p = c_p(K) = \#\{\text{ノルムが } p \text{ である } K \text{ の素イデアル}\}$$

と置く。

命題 2-2 「 $\lim_{N \rightarrow \infty} \frac{1}{\pi(N)} \sum_{p: \text{素数} \leq N} c_p$
 $= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} \log(p) \cdot c_p = 1$ が成り立つ。」 \odot

証明 三井 [3] p.65 定理 3. 4. 7 より

$$\sum_{\mathfrak{p}: K \text{ の素イデアル } N\mathfrak{p} \leq N} \log(N\mathfrak{p}) = N + O(N \cdot \exp^{-c \cdot \sqrt{\log N}})$$

がわかる。

これと、命題 2-1 よりこの命題を得る。q.e.d.

上の命題より次を得る。

系 2-2

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \equiv 1 \pmod{4}, < N} \log(p)$$

$$= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \equiv 3 \pmod{4}, \leq N} \log(p) = 1/2,$$

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \equiv 1 \pmod{8}, \leq N} \log(p) = 1/4 \quad \odot$$

証明

$K = \mathbb{Q}(\sqrt{-1})$ 及び、 $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ の時に上の命題を使えば良い。q.e.d.

§ 3 佐藤予想

記号 Q 上定義された楕円曲線 E に対して

$$\begin{aligned} c_m &= \lim_{N \rightarrow \infty} \frac{1}{\pi(N)} \sum_{p: \text{素数} \leq N} b(p, m)/p^{m/2} \\ &= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} \log(p) \cdot b(p, m)/p^{m/2}, (m \geq 1) \end{aligned}$$

とおく。(等号は $|b(p, m)| < p^{m/2}$ と命題 1-1 よりわかる。)

このとき、山本 [4] より次がわかる。

命題 3-1 「 E が CM-型の時、 $c_{2m} = (-1)^m, c_{2m-1} = 0, (m \geq 1)$ が成り立つ。」 \odot

予想 3-1 (佐藤予想) 「 E が CM-型でない時、

$$c_m = \begin{cases} -1 & m=2 \text{ の時} \\ 0 & \text{その他の時} \end{cases}$$

が成り立つ。」 \odot

この予想により次がわかる。

命題 3-2 「佐藤予想の下で

$$\lim_{s \rightarrow 1+0} (s-1) \cdot f_2(s) = 1/2 \text{ がわかる。} \quad \odot$$

証明 $-1 = c_2 = \frac{1}{N} \sum_{p: \text{素数} \leq N} \log(p) \cdot b(p, 2)$ より

$$g(s) = \sum_{p: \text{素数}} \log(p) \cdot B(p, 2) \cdot p^{-1-s} \text{ とおくと、}$$

命題 1-1 より $\lim_{s \rightarrow 1+0} (s-1) \cdot g(s) = -1$ がわかる。

また、 $f_2(s) = -g(2s-1)$ より上がわかる。q.e.d.

§ 4 $Q(T)$ -rank

記号 $f(X) \in \mathbb{Z}[X]$ を重根を持たない monic な三次式とする。

また、 $f(X) = (X-a)(X-\beta)(X-\gamma) \quad (a, \beta, \gamma \in \overline{\mathbb{Q}})$ とおく。

ここでは、以下を示す。

命題 4-1 「 $\varepsilon: Y^2=f(X)+T$ の $Q(T)$ -rank は 0。」 \odot

命題 4-2 「 $\varepsilon: Y^2=f(X)+T^2$ の $Q(T)$ -rank は $f(X)$ が既約、二次式 \times 一次式に分解、一次式 \times 一次式 \times 一次式に分解の時それぞれ 0, 1, 2 となる。」 \odot

補題 (塩田 [1]) 「 k を標数が 2, 3 でない完全体とする。 b_1, b_2, b_3 を相異なる K の元とする。このとき、 $K=k(T)$ 上定義された楕円曲線 $Y^2=(X-b_1)(X-b_2)(X-b_3)+T^2$ の rank は 2 で、torsion はなく、その生成元は $P_1=(b_1, T), P_2=(b_2, T)$ である。」 \odot

命題 4-1 の証明 $K=Q(\sqrt{T}, \alpha, \beta, \gamma)$ とおく。 σ を $\sqrt{T} \rightarrow -\sqrt{T}, \alpha, \beta, \gamma$ 不変をみたす $Gal(K/Q(T))$ の元とする。

$(n_1P_1+n_2P_2)^\sigma = n_1P_1^\sigma+n_2P_2^\sigma = -n_1P_1-n_2P_2$ より $\varepsilon(K)$ の元で σ 不変な元は ∞ のみであることがわかる。

命題 4-2 の証明 $f(X)$ が三つの一次式の積に分かれる時、 $(\alpha, \beta, \gamma \in \overline{Q})$ 上の補題より rank = 2 が直ちにわかる。 $f(X)$ が二次式と一次式の積に分かれる時、 $(\alpha, \beta, \gamma \in \overline{Q}$ とおく) $K=Q(\beta, T), \sigma$ を $\beta \rightarrow \gamma$ を満たす $Gal(K/Q(T))$ の元とする。

$(n_1P_1+n_2P_2)^\sigma = n_1P_1^\sigma+n_2P_2^\sigma = n_1P_1-n_2P_2$ より $\varepsilon(K)$ の元で σ 不変な元は $P_1 (\in \varepsilon(Q(T)))$ の整数倍とかけることがわかる。 $f(X)$ が既約の時、 $(\alpha, \beta, \gamma \in \overline{Q}$ である) $K=Q(\alpha, \beta, T), \sigma$ を $\alpha \rightarrow \beta, \beta \rightarrow \gamma$ を満たす $Gal(K/Q(T))$ の元とする。

$(n_1P_1+n_2P_2)^\sigma = n_1P_1^\sigma+n_2P_2^\sigma = n_1P_2+n_2(-P_1-P_2) = -n_2P_1-(n_1+n_2)P_2$ より $\varepsilon(K)$ の元で σ 不変な元は ∞ のみであることがわかる。 q.e.d.

§ 5 定理 2 の証明

$\varepsilon: Y^2=f(X)+T^2$ とする。

補題 「 $f(X) \bmod p$ が重根をもたない p に対して $-A_p = \begin{cases} 2, & f(X) \bmod p \text{ が三つの一次式に分解するとき} \\ 0, & f(X) \bmod p \text{ が二次式} \times \text{一次式と分解するとき} \\ -1, & f(X) \bmod p \text{ が既約のとき} \end{cases}$ が成り立つ。」 \odot

証明 $-pA_p = \sum_{t=0}^{p-1} -a_p(E_t) = \# \{(x, y, t) \in F_p^3 \mid y^2 = f(x) + t^2\} - p^2 = (\sum_{x=0}^{p-1} \# \{(y, t) \in F_p^2 \mid y^2 = f(x) + t^2\}) - p^2 = (\sum_{x=0}^{p-1} \# \{(y, t) \in F_p^2 \mid (y-t)(y+t) = f(x)\}) - p^2$ である。また、任意の F_p の元 a に対して

$$\# \{(y, t) \mid (y-t)(y+t) = a\} = \begin{cases} 2p-1, & \text{if } a=0 \\ p-1, & \text{if } a \neq 0 \end{cases}$$

より $-pA_p$ は $\begin{cases} 3(2p-1) + (p-3)(p-1) - p^2 & f(X) \bmod p \text{ が三つの一次式に分解するとき} \\ 2(2p-1) + (p-2)(p-1) - p^2 & f(X) \bmod p \text{ が二次式} \times \text{一次式と分解するとき} \\ p \cdot p - p^2 & f(X) \bmod p \text{ が既約のとき} \end{cases}$

となり題意を得る。 q.e.d.

この補題より $f(X)$ が三つの一次式に分解するとき $A_p = -2$ がわかり系 2-1 より $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} -\log(p) \cdot A_p = 2$ がわかり証明ができる。

以下、その他の場合についてしめす。 $f(X) = (X-\alpha)(X-\beta)(X-\gamma)$ とおく。また、 α, β, γ をうまく取り替えることによって $\beta, \gamma \in \mathbb{Q}$ としておく。また、代数体 $Q(\beta)$ を K とおく。また、素数 p に対して $c_p = \# \{\text{体 } K \text{ 内で } p \text{ 上にある一次の素イデアル}\}$ とする。

case 1 $\alpha, \beta, \gamma \in \mathbb{Q}, Q(\alpha, \beta, \gamma)/\mathbb{Q}$ 六次 S_3 拡大のとき。 $f(X) \bmod p$ が重根をもたない p に対して $c_p = 3 \Leftrightarrow f(X) \bmod p$ が三つの一次式に分解 $\Leftrightarrow -A_p = 2$ $c_p = 1 \Leftrightarrow f(X) \bmod p$ が二次式 \times 一次式に分解 $\Leftrightarrow -A_p = 0$ $c_p = 0 \Leftrightarrow f(X) \bmod p$ が既約 $\Leftrightarrow -A_p = -1$ より $-A_p = c_p - 1$ がわかる。よって、命題 2-2 より $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} -\log(p) \cdot A_p = \lim_{N \rightarrow \infty} \frac{1}{N} \{ \sum_{p: \text{素数} \leq N} \log(p) \cdot c_p - \sum_{p: \text{素数} \leq N} \log(p) \} = 1 - 1 = 0$

がわかる。

case 2 $\alpha, \beta, \gamma \in \mathbb{Q}, Q(\alpha, \beta, \gamma)/\mathbb{Q}$ 三次巡回拡大のとき。

$f(X) \bmod p$ が重根をもたない p に対して同様に $-A_p = c_p - 1$ がいえ題意が証明できる。

case 3 $\alpha \in \mathbb{Q}, \beta, \gamma \in \mathbb{Q}, Q(\alpha, \beta, \gamma)/\mathbb{Q}$ 二次拡大のとき。 $f(X) \bmod p$ が重根をもたない p に対して同様に $-A_p = c_p$ がいえ題意が証明できる。

§ 6 定理 4 の証明

補題 (Ireland-Rosen [5] p.307 Theorem 5) 「 Q 上定義された楕円曲線 $E: Y^2 = X^3 - DX$ の a_p は $2D$ を割らない素数 p に対して

$$a_p = \begin{cases} 0 & p \equiv 3 \pmod{4} \\ \frac{0}{(D/\pi)_4} \pi + \frac{(D/\pi)_4}{\pi} & p \equiv 1 \pmod{4} \end{cases}$$

である。

ただし $p \equiv 1 \pmod{4}$ のとき $p = \pi \bar{\pi}$, $\pi \equiv 1 \pmod{2+2\sqrt{-1}}$ とおく。」○

とくに、 $D=1$ のとき

$$a_p = \begin{cases} 0 & p \equiv 3 \pmod{4} \\ -2b & p \equiv 1 \pmod{4} \end{cases}$$

である。

ただし $p \equiv 1 \pmod{4}$ のとき $p = a^2 + b^2$ a : 偶数、 b : 奇数とする。

補題

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数}=1 \pmod{4}, \leq N} 4b^2 \cdot \log(p)/p = 1 \quad \circ$$

証明 CM-型の楕円曲線 $Y^2 = X^3 - X$ にたいして命題 2-1 より

$$-1 = c_2 = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} b(p, 2) \cdot \log(p)/p$$

がわかる。また $b(p, 2) = a_p^2 - 2p$ よりこの式は、

$$\begin{aligned} &= \left(\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} a_p^2 \cdot \log(p)/p \right) - 2 \\ &= \left(\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数}=1 \pmod{4}, \leq N} a_p^2 \cdot \log(p)/p \right) - 2 \end{aligned}$$

となり題意がわかる。q.e.d.

以下、定理 4 を示す。

$$\begin{aligned} &\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{p: \text{素数} \leq N} -\log(p) \cdot A_p \\ &= \frac{1}{N} \sum_{p: \text{素数}=1 \pmod{4}, \leq N} 4b^2 \cdot \log(p)/p \\ &\quad + \frac{1}{N} \sum_{p: \text{素数}=1 \pmod{8}, \leq N} 4 \cdot \log(p) \\ &\quad + \frac{1}{N} \sum_{p: \text{素数}=3 \pmod{4}, \leq N} -2 \cdot \log(p) \end{aligned}$$

であり、この値は上の補題と系 2-2 より

$1 + 4 \cdot 1/4 - 2 \cdot 1/2 = 1$ となる。

よって、定理 4 の証明が終わった。

§ 7 Tate 予想

ここでは、Tate の予想と我々の予想との関係について述べる。

Tate 予想 (cf. [6] p.104 Conjecture 2)

「 V を代数体 k 上定義された smooth な surface とする。また、 $\zeta_{k,V}(s)$ をその Hasse-zeta function とする。このとき、 V の Neron-Severi 群 $NS(k)$ の k -rank は $\zeta_{k,V}(s)$ の $s=2$ での零点の位数に等しい。」

我々が考察している $Q(T)$ -上定義された楕円曲線は Q 上定義された (必ずしも smooth ではない) 楕円曲面とすることができる。一方、代数体 k 上定義された smooth な楕円曲面 V についてその Neron-Severi 群の k -rank はそれを $k(T)$ 上定義された楕円曲線と考えたときの $k(T)$ -有理点の rank から簡単に計算できる。よって、上の予想は $Q(T)$ -上定義された楕円曲線が Q 上定義された smooth な楕円曲面である場合においてその $Q(T)$ -rank がその zeta 関数の零点の位数によって書かれるという予想となり、このような場合においては我々以前に既に予想が成されていたことに注意しておく。よって、我々の予想の新しい点は

1. 楕円曲線が Q 上では smooth でない楕円曲面となる場合にも有効。
 2. 実験が容易である。
- という点である。

参考文献

1. T.Shioda, Construction of elliptic curves with high-rank via the invariants of the Weyl groups, J.Math.Soc Japan 43 no 4 1991 673-719pp
2. M.Kuwata, Mordell-Weil groups and elliptic K3-surfaces, Dr.Thesis of Brown University 1989
3. 三井孝美 解析的数論 岩波 1989
4. 山本芳彦 SATO 予想について Master Theses Osaka University 1964
5. K.Ireland and M.Rosen, A Classical Introduction to Modern Number Theory, Springer GTM 1972
6. J.Tate, Algebraic cycles and poles of zeta functions, Arithmetic Algebraic Geometry, ed. Schilling, Harper and Row (1965) p.93-111.