Recovering short generators via negative moments of Dirichlet L-functions

名古屋大学大学院多元数理科学研究科 * 戸澗　勇一郎 †
Yuichiro Toma
Graduate School of Mathematics, Nagoya University

概要

格子問題に基づく暗号方式は, 格子上の計算問題の難しさを安全性の根拠とする暗号方式である. いくつかの代数的イデアル格子ベースの暗号システムは, 与えられた主イデアルの短い生成元を見つけることの計算困難性に依拠している. このような格子暗号の安全性評価を行う上では, これらの格子問題に対する攻撃手法の効率性を調べることが不可欠である. EUROCRYPT2016 において, Cramer, Ducas, Peikert および Regev は 1 の原始 q 乗根 ξ_q (q は素数冪) に対する円分体 $\mathbb{Q}(\xi_q)$ における主イデアルの短い生成元を復元する古典アルゴリズムを提案した. 本講演では, $s = 1$ での Dirichlet L 関数の負冪モーメントを計算することで, 特別な場合において, Cramer, Ducas, Peikert, Regev によるアルゴリズムを改良した結果について述べる (詳細は [7, 8]). 本研究は名古屋大学の Iu-Iong Ng 氏との共同研究である.

§1. 導入

本稿では, 断りのない限り $q = p^\ell$ (> 2) は素数冪とする. また, ξ_q を 1 の原始 q 乗根とし, $K = \mathbb{Q}(\xi_q)$ を円分体とする. このとき K の拡大次数は $[K : \mathbb{Q}] = \varphi(q)$ で与えられる. 円分体において K の Dedekind ゼータ関数 $\zeta_K(s)$ は

$$\zeta_K(s) = \sum_{\mathfrak{a} \in \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\chi \bmod q} L(s, \chi)$$

* 〒464-8602 愛知県名古屋市千種区不老町
† m20034y@math.nagoya-u.ac.jp

である．ここで, $L(s,\chi)$ は法 q の Dirichlet L 関数である．また, K の対数埋め込みを以下のように定める．

$$\begin{array}{rccc} \mathrm{Log}\colon & K^\times & \longrightarrow & \mathbb{R}^{\frac{\varphi(q)}{2}} \\ & \cup & & \cup \\ & a & \longmapsto & (\log(|\sigma_j(a)|))_{j\in G} \end{array}$$

ここで $G=\mathbb{Z}_q^\times/\{\pm 1\}$ であり, σ_j は K の複素埋め込みである．この写像により単数群はユークリッド空間に埋め込まれる．さらに Dirichlet の単数定理により, $\mathrm{Log}(O_K^\times)$ は $\mathbb{R}^{\frac{\varphi(q)}{2}}$ 内の格子（log-unit lattice）を形成する．

整数環の単数群 $O_K^\times$ の部分群である cyclotomic unit group を以下のように定義する．

$$\mathcal{C} := \left\langle \pm\xi_q, b_j = \frac{\xi_q^j - 1}{\xi_q - 1} \;\middle|\; j \in G\setminus\{1\} \right\rangle.$$

先ほど定義した Log を用いると, cyclotomic unit group $\mathcal{C}$ の対数埋め込みは

$$\mathrm{Log}(\mathcal{C}) = \{\mathrm{Log}(b_j) \mid j\in G\}$$

により与えられ, $\mathrm{Log}(\mathcal{C})$ は $\mathrm{Log}(O_K^\times)$ の部分格子となる．本論文では, この包含関係の指数 $[\mathrm{Log}(O_K^\times) : \mathrm{Log}(\mathcal{C})]$ が小さいと仮定する．また, $j\in G\setminus\{1\}$ に対して $\mathbf{b}_j := \mathrm{Log}(b_j)$ とし, $\mathbf{b}_j^\vee$ は $\mathbf{b}_j$ の dual basis であり, $\langle \mathbf{b}_j^\vee, \mathbf{b}_{j'}\rangle = \delta_{j,j'}$ で与えられるものとする．

§2. Short Generator problem

Short Generator problem (SGP) とは, 与えられた整数環の主イデアルの生成元をもとに十分に短い生成元を復元する問題である．SGP の研究の背景の一つとして格子暗号があり, 格子暗号は近年急速に進化している量子コンピュータでも解くことが難しい耐量子計算機暗号の候補の一つであるが, 一部の格子問題に対しては, 特定の制約や緩和条件のもとで効率的な量子アルゴリズムが存在する．格子暗号の安全性評価のためには, こうした効率的なアルゴリズムを見つけることが重要であり, 2016 年に Cramer, Ducas, Peikert, Regev [4] (以下, CDPR16) は, q が素数冪の円分体 $\mathbb{Q}(\xi_q)$ の場合に, SGP を多項式時間で解く古典アルゴリズムを与えた．つまり, q が素数冪の円分体 $\mathbb{Q}(\xi_q)$ の場合は, 量子アルゴリズムでなくても, SGP ベースの格子暗号は解かれてしまう．

CDPR16 の結果をより詳し述べると, CDPR16 は与えられた O_K の主イデアル hO_K の生成元 h から, $\|\mathrm{Log}(g)\|$ が十分に短くなるような別の生成元 g 見つける古典アルゴリズムを提案した．ただし, $\|\cdot\|$ は $\mathbb{R}^{\frac{\varphi(q)}{2}}$ の Euclid ノルムである．このとき, CDPR16 のアルゴリズムの成功確率は $1-(\varphi(q)-2)e^{-\frac{t}{2}}$, ただし, $t=\frac{1}{2}\|\mathbf{b}_j^\vee\|^{-1}$ で与えられる．このア

ルゴリズムが十分機能することを保証するには, $\|\mathbf{b}_j^\vee\|$ の大きさを評価する必要があるが, CDPR16 は

$$\|\mathbf{b}_j^\vee\| = \sqrt{\frac{8}{\varphi(q)} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi \left|L(1,\chi)\right|^2}}, \tag{1}$$

であることを示している. ここで, f_χ は χ の conductor である. CDPR16 は $L(1,\chi)$ の lower bound

$$|L(1,\chi)| \gg \begin{cases} \frac{1}{\log f_\chi} & (\chi : \text{non quadratic}), \\ \frac{1}{\sqrt{f_\chi}} & (\chi : \text{quadratic}) \end{cases}$$

を用いれば, $\|\mathbf{b}_j^\vee\| \ll \frac{\sqrt{\ell}\log q}{\sqrt{\varphi(q)}}$ であり, CDPR16 のアルゴリズムの成功確率は $1-(\varphi(q)-2)e^{-\frac{t}{2}}$, ただし, $t \gg \frac{\sqrt{\varphi(q)}}{\sqrt{\ell}\log q}$ が従う. さらに, GRH を仮定すれば,

$$|L(1,\chi)| \gg \frac{1}{\log\log f_\chi}$$

が成り立つため, GRH 仮定下では, それぞれ $\|\mathbf{b}_j^\vee\| \ll \frac{\sqrt{\ell}\log\log q}{\sqrt{\varphi(q)}}$ と $t \gg \frac{\sqrt{\varphi(q)}}{\sqrt{\ell}\log\log q}$ が導かれる.

では, $L(1,\chi)$ の lower bound を用いるのではなく, $L(1,\chi)$ の離散モーメントを直接求めることは可能だろうか. もし q が奇素数であれば, $\chi \neq \chi_0$ に対して $f_\chi = q$ が成り立つので,

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi \left|L(1,\chi)\right|^2} = \frac{1}{q} \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{\left|L(1,\chi)\right|^2}$$

であるため,

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{\left|L(1,\chi)\right|^2}, \qquad \sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi \left|L(1,\chi)\right|^2}$$

について解説する.

§3. Dirichlet L 関数の負の離散モーメント

まず, 負のモーメントに限らず, Dirichlet L 関数の $s=1$ での一般的な離散のモーメントについて述べる. Paley, Selberg ([1] 参照) は q を素数として法 q の Dirichlet L 関数の

$s=1$ での離散モーメントの漸近式

$$\sum_{\substack{\chi \bmod q \\ \chi\neq\chi_0}} |L(1,\chi)|^2 = \zeta(2)q + O\left((\log q)^2\right)$$

を与えることで, $\mathbb{Q}(\xi_q)$ の類数の評価を与えている. こうした方向から正のモーメントについては多く研究されてきた. 一方で, 負のモーメントについては同様の動機が存在せず, これまで負の離散モーメントの漸近挙動については, 研究されていなかった.

CDPR16 のアルゴリズムへの応用を考える上では $q=p^\ell$ の場合で十分であるが, Dirichlet L 関数の負の 2 次の離散モーメントについては q を素数冪に限定しなくても漸近挙動が得られた.

Theorem 1. 正の整数 q に対して

$$\sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1} \varphi(q) + O\left(\exp\left(C\frac{\log q}{\log\log q}\right)\right) + O\left(\delta_1 (1-\beta_1)^{-1}\left((\log q)^2 + (1-\beta_1)^{-1}\right)\right)$$

が成り立つ. ここで, $C>0$ は定数であり, β_1 は *Siegel* 零点, そして β_1 が存在するとき $\delta_1=1$ であり, 存在しないとき $\delta_1=0$ である.

Siegel の定理から, Siegel 零点が存在する場合でも $1-\beta_1 \geq C(\varepsilon)q^{-\varepsilon}$ が分かっている. よって

$$\sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1} \varphi(q) + O_\varepsilon\left(q^\varepsilon\right)$$

が成り立つ.

また, CDPR16 の結果とは直接関係ないが, GRH 仮定下で正の整数 k に対して

$$\sum_{\substack{\chi\neq\chi_0 \\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^{2k}} = \frac{C(k)}{2}\varphi(q) \prod_{p\mid q}\left(1+\frac{\binom{k}{1}^2}{p^2}+\cdots+\frac{\binom{k}{k}^2}{p^{2k}}\right)^{-1} + O\left(q^\varepsilon\right)$$

が成り立つ. ここで

$$C(k) = \prod_p \left(1+\frac{\binom{k}{1}^2}{p^2}+\cdots+\frac{\binom{k}{k}^2}{p^{2k}}\right)$$

である. この結果は, Zhang-Wang [10] による

$$\sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} |L(1,\chi)|^{2k} = \varphi(q) \sum_{n=1}^{\infty} \frac{d_k^2(n)}{n^2} + O\left(\exp\left(2k \frac{\log q}{\log\log q}\right)\right)$$

の負の類似とも考えることができる.

次に, conductor が分母に含まれる負の離散モーメントの場合は, いくつか制限を設ける必要がある.

Theorem 2. 素数冪 $q = p^\ell$ に対して, 法 q の *Dirichlet* L 関数が *Siegel* 零点を持たないとする. このとき,

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi |L(1,\chi)|^2} = \frac{\zeta(2)}{2\zeta(4)} \frac{(p-1)^2}{p^2+1} \ell + O\left(\frac{1}{\log p}\right) + O\left(\frac{\ell^2 (\log p)^2 (\log \ell + \log\log p)^2}{p}\right)$$

が $\ell = o\left(\frac{p}{(\log p)^4}\right)$ の制限のもとで成り立つ.

素数冪 $q = p^\ell$ が $q \to \infty$ となるのは, (1) 素数 p を固定し, $\ell \to \infty$, (2) 冪 ℓ を固定し, $p \to \infty$, (3) $p, \ell \to \infty$ の 3 つの場合が存在する. ここで, 制限 $\ell = o\left(\frac{p}{(\log p)^4}\right)$ は (2) の場合と (3) で ℓ が p に比べて小さい時の場合が当てはまる.

もし, $\ell = o\left(\frac{p}{(\log p)^4}\right)$ が成り立たない場合, すなわち $\ell \gg \frac{p}{(\log p)^4}$ の場合には, 第 2 誤差項の大きさが主要項の大きさを超えてしまう. これは, 分母にある conductor の寄与により主要項が小さくなるためである. そのため, 上記のような漸近式は成り立たず,

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi |L(1,\chi)|^2} \ll \frac{\ell^2 (\log p)^2 (\log \ell + \log\log p)^2}{p}$$

しか得られない. しかしながら, この upper bound はわずかではあるが, $L(1,\chi)$ の lower bound を用いて得られる評価より良い評価を与えている. 実際, $|L(1,\chi)|$ の lower bound を用いて得られるのは

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} \frac{1}{f_\chi |L(1,\chi)|^2} \ll \ell^3 (\log p)^2$$

までであるので, $\ell \gg \frac{p}{(\log p)^4}$ の場合においても, CDPR16 の結果より良い評価が得られている.

§4. log-cyclotomic unit 格子の双対基底

以下では Dirichlet L 関数の負の離散モーメントの漸近式を, log-cyclotomic unit 格子の双対基底の評価に応用する. 式 (1) と, Theorem 1より, 十分大きな素数 q に対して,

$$\|\mathbf{b}_j^\vee\| = \sqrt{\frac{4\zeta(2)}{\zeta(4)}}\frac{1}{\sqrt{\varphi(q)}}\left(1+O_\varepsilon\left(q^{-1+\varepsilon}\right)\right) \qquad (q\to\infty)$$

が成り立つ. この $\|\mathbf{b}_j^\vee\|$ の漸近式より, 素数 q が十分大きいとき, CDPR16 自身が示した彼らアルゴリズムの成功確率の下界を $1-(\varphi(q)-2)e^{-\frac{t}{2}}$, ただし, $t=\frac{1}{4}\sqrt{\frac{\zeta(4)}{\zeta(2)}\varphi(q)}\left(1+O\left(q^{-1+\varepsilon}\right)\right)$ に改良することが出来る.

また, $q=p^\ell>2$ が素数冪のときは, 法 q の Dirichlet L 関数が Siegel 零点を持たないことと, $\ell=o\left(\frac{p}{(\log p)^4}\right)$ であると仮定する. このとき,

$$\|\mathbf{b}_j^\vee\| = \sqrt{\frac{4\zeta(2)}{\zeta(4)}\frac{\ell}{\varphi(p^\ell)}}\left(1+o\left(1\right)\right) \qquad (q\to\infty)$$

が成り立つ. したがって, Siegel 零点の非存在と $\ell=o\left(\frac{p}{(\log p)^4}\right)$ の仮定下で, CDPR16 自身が示した彼らのアルゴリズムの成功確率の下界を $1-(\varphi(q)-2)e^{-\frac{t}{2}}$, ただし, $t=\frac{1}{4}\sqrt{\frac{\zeta(4)}{\zeta(2)}\frac{\varphi(p^\ell)}{\ell}}\left(1+o\left(1\right)\right)$ に改良することが出来る.

§5. 今後の課題

最後に, Riemann ゼータ関数の負のモーメントの結果について紹介する. Riemann ゼータ関数の正のモーメントのオーダーは Lindelöf 予想との関連もあり, Hardy-Littlewood の時代から広く研究されている. 特に, 臨界線上のモーメントについては, Keating-Snaith [6] より, $k\geq 0, T\geq 1$ に対して

$$\int_0^T \left|\zeta(1/2+it)\right|^{2k}dt \sim \frac{c_k g_k}{(k^2)!}T(\log T)^{k^2}$$

という漸近式が予想されている. ただし,

$$c_k=\prod_p\left(\left(1-\frac{1}{p}\right)^{k^2}\sum_{\alpha=0}^{\infty}\frac{\tau_k(p^\alpha)^2}{p^\alpha}\right), \quad g_k=(k^2)!\prod_{j=0}^{k-1}\frac{j!}{(j+k)!}.$$

一方で, 負のモーメントについての研究は比較的新しく, 1989 年に Gonek により負のモーメントのオーダーが予想されている. 正の実数 $0 < \alpha \leq 1$ と $k > 0$ に対して

$$I_{-k}(\alpha, T) := \frac{1}{T} \int_0^T \left| \zeta(\frac{1}{2} + \alpha + it) \right|^{-2k} dt$$

とする.

Conjecture 3. 正の実数 $\alpha > 0$ が $\frac{1}{\log T} \leq \alpha \leq 1$ のとき,

$$I_{-k}(\alpha, T) \asymp \left(\frac{1}{\alpha} \right)^{k^2}$$

が成り立つ. また, $0 < \alpha \leq \frac{1}{\log T}$ のとき,

$$I_{-k}(\alpha, T) \asymp \begin{cases} (\log T)^{k^2} & \text{if } k < \frac{1}{2}, \\ \left(\log \frac{e}{\alpha \log T} \right) (\log T)^{k^2} & \text{if } k = \frac{1}{2} \end{cases}$$

が成り立つ.

現時点では, Riemann ゼータ関数の零点が $\frac{1}{2} + \alpha$ 上にあることを否定できないため, 負のモーメントを評価するためには RH を仮定する. 実際, Gonek 自身 [5] は RH 仮定下で, $I_{-k}(\alpha, T)$ の予想と一致する lower bound を与えた. 一方, Bui-Florea [3] は Gonek 予想のオーダーには及ばないものの, RH 仮定下で非自明な upper bound を与えている. Gonek 予想の応用として, Mertens 関数の upper bound の評価の改良できることが挙げられる. Mertens 関数

$$M(x) := \sum_{n \leq x} \mu(n)$$

が $M(x) \ll x^{\frac{1}{2}+\varepsilon}$ であることと, RH が同値であることが知られている. 2008 年に Balazard-de Roton [2] は RH 仮定下で,

$$M(x) \ll x^{\frac{1}{2}} \exp\left((\log x)^{\frac{1}{2}} (\log\log\log x)^{\frac{5}{2}+\varepsilon} \right)$$

が成り立つことを示している. Bui-Florea [3] は RH と Gonek 予想仮定下で

$$M(x) \ll x^{\frac{1}{2}} (\log x)^{\frac{1}{4}}.$$

まで改良できることを示した. これは, Gonek 予想が非常に強い予想であることの根拠を与えており, 実際, Mertens 関数の評価については, 同じく非常に強い予想である特殊な場合の “弱い”Gonek-Hejhal 予想仮定下よりも良い評価をもたらす.

ここで, Gonek-Hejhal 予想とは, Riemann ゼータ関数の非自明零点 $\rho = \beta + i\gamma$ に対して

$$J_\lambda(T) := \sum_{0<\gamma\leq T} |\zeta'(\rho)|^{2\lambda} \asymp T(\log T)^{(\lambda+1)^2}$$

が任意の $\lambda > -\frac{3}{2}$ に対して成り立つことを主張する予想である. N. Ng [9] は RH と特殊な場合の “弱い”Gonek-Hejhal 予想 $J_{-1}(T) \ll T$ を仮定のもとで

$$M(x) \ll x^{\frac{1}{2}}(\log x)^{\frac{3}{2}}$$

が成り立つことを示している (注: 紙面の都合上, 本稿では “弱い”Gonek-Hejhal 予想と呼んでいるが, $J_{-1}(T) \ll T$ が一般にそう呼ばれているわけではない). Gonek-Hejhal 予想は Riemann ゼータ関数に対する一位零点予想より強い予想であるが, Gonek 予想を仮定した方が $J_{-1}(T) \ll T$ を仮定するのに比べ, $\log x$ の冪が若干良くなっている.

一方で, Gonek 予想と Gonek-Hejhal 予想との直接的なつながりは分かっておらず, これら二つの予想の関係性を明らかにすることが今後の課題の一つである.

Acknowledgements. 本稿は 2024 年度 RIMS 共同研究（公開型）「解析的整数論とその周辺」における筆者の講演を元に作成されたものです. 講演の機会を与えてくださった中筋麻貴先生, 谷口隆先生に感謝申し上げます. 本研究は, 日本学術振興会特別研究費 (課題番号:24KJ1235) の助成を受けたものです.

参考文献

[1] N.C. Ankeny and S. Chowla, The class number of the cyclotomic fieıd, Canad. J. Math., **3** (1951), 486–494.

[2] M. Balazard and A. de Roton, Notes de lecture de l’article “Partial sums of the Möbius function” de Kannan Soundararajan, preprint, arXiv:0810.3587.

[3] H. M. Bui, A. Florea, Negative moments of the Riemann zeta-function, J. Reine Angew. Math. **806** (2024), 247—288.

[4] R. Cramer, L. Ducas, C. Peikert, O. Regev, Recovering short generators of principal ideals in cyclotomic rings, in: Proceedings of the 35th Annual International Conference on Advances in Cryptology—EUROCRYPT 2016, vol. 9666, Springer-Verlag, Berlin, Heidelberg, 2016, pp. 559—585.

[5] S. M. Gonek, On negative moments of the Riemann zeta-function, Mathematika **36** (1989), no. 1, 71—88.

[6] J. P. Keating, N. C. Snaith, Random matrix theory and $\zeta(1/2 + it)$, Comm. Math. Phys. **214** (2000), no. 1, 57–89.

[7] I.-I. Ng, Y. Toma, Recovering short generators via negative moments of Dirichlet L-functions, arXiv:2405.13420.

[8] I.-I. Ng, Y. Toma, Mean square of inverses of Dirichlet L-functions involving conductors, arXiv:2501.11316.

[9] N. Ng, The distribution of the summatory function of the Möbius function, Proc. Lond. Math. Soc. (3) **89** (2004), no. 2, 361–389.

[10] W. Zhang, W. Wang, An exact calculating formula for the $2k$-th power mean of L-functions, JP Jour. Algebra. Number Theory and Appl. **2** (2002) no. 2, 195–203.