CLASSICAL NUMBER THEORY AND RATIONAL POINTS ON ELLIPTIC CURVES: OBSERVATION NOTE

KAZUMA MORITA

Abstract. In this note, we shall give a self-righteous observation on rational points on elliptic curves from the classical number theoretic view point.

1. Rational points on arithmetic curves

It is well-known that, as the genus of curves gets higher, the number of rational points (or integral points) on arithmetic curves decreases. Especially, we shall investigate how rational points (or integral points) behave when they move from a curve of genus 0 to a curve of genus 1.

2. L-function of elliptic curves and Dedekind zeta function

For an elliptic curve E over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture predicts that the rank of Mordell-Weil group $E(\mathbb{Q})$ is equal to the order of the zero of $L(E,s)$ at $s=1$. On the other hand, for an algebraic number field K over $\mathbb{Q}$, there is a similar formula which states that the number of generators of the unit group $\mathcal{O}_K^*$ can be described by the order of the zero of Dedekind zeta function $\zeta_K(s)$ at $s=0$. In particular, when K is a real quadratic extension of $\mathbb{Q}$, the number of generators of the unit group $\mathcal{O}_K^*$ is equal to 1 and these unit elements correspond to integral points on a quadratic curve $x^2-Dy^2=1$ (Pell equation). It seems to me that, when they move from this quadratic curve to an elliptic curve, these integral points may turn into rational points.

3. Rational points and unit elements

3.1. **Some histories.** Traditionally, units elements have played an important role for calculating arithmetic invariants and have been closely related to rational points. For example, in proving the Dirichlet's Unit Theorem, finding one of generators of $\mathcal{O}_K^*$ is equivalent to finding an integral point on some parallelogram. Furthermore, Siegel's Theorem on the finiteness of integral points on $y^2=f(x)$ ($f(x)\in\mathbb{Q}[x], \deg(f(x))\geq 3$) is deduced from the finiteness of certain unit elements,...et al. In a modern language, unit elements such as elliptic units

Date: April 14, 2016.

1991 *Mathematics Subject Classification.* 11F03, 11G05, 11G40.

Key words and phrases. classical number theory, elliptic curves, L-functions.

or Kato's elements form an Euler system and are used to calculate the L-value which is closely related to rational points.

This is one of the reasons why it seem to me that integral points on a Pell equation $x^2 - Dy^2 = 1$ which represent unit elements of $\mathcal{O}_K^*$ may be converted into rational points on an elliptic curve. Furthermore, this conversion corresponds to the fact that, as the genus of curves gets higher, the number of rational points (or integral points) on arithmetic curves decreases.

3.2. **From Pell equations to an elliptic curve.** For simplicity, assume that K is a real quadratic extension of $\mathbb{Q}$ and that E is an elliptic curve over $\mathbb{Q}$ whose Mordell-Weil group is of rank 1. Let χ_K (resp. $\chi_{\mathbb{Q}}$) denote the Dirichlet character such that we have $\zeta(s)L(\chi_K, s) = \zeta_K(s)$ (resp. $\zeta(s)L(\chi_{\mathbb{Q}}, s) = \zeta_{\mathbb{Q}}(s)$). Furthermore, take the rational newform f of weight 2 such that we have $L(E, s) = L(f, s)$. Then, we have

$$(*) \quad L(\chi_K, 0)L(\chi_{\mathbb{Q}}, 0) = L(\chi_K(-1), 1)L(\chi_{\mathbb{Q}}(-1), 1) \sim L(f, 1) = L(E, 1)$$

where $\sim$ means that both sides have the same order and both leading terms are connected by a homotopy method.

Remark

(1) This identification is a very rough one and we may consider a more refined version which preserves arithmetic invariants such as conductors. In those cases, it will be quite interesting to study the orders of Selmer groups.
(2) The unit elements of $\mathbb{Z}^*$ can be corresponded to the integral points on the Pell equation of the form $x^2 - n^2y^2 = 1$ ($n \in \mathbb{N}$) and this equation has only trivial integral points.

By the formula $(*)$ above, we can regard that two Pell equations which come from unit groups $\mathcal{O}_K^*$ and $\mathbb{Z}^*$ melt into the elliptic curve E over $\mathbb{Q}$ whose Mordell-Weil group is of rank 1 and that the integral points on one Pell equation turn into the (non-torsion) rational points on the elliptic curve E.

Remark

(1) Since the L-function $L(\mathbb{P}_1, s)$ is trivial, one cannot obtain any interesting information by considering two $L(\mathbb{P}_1, s)$. In this note, we make use of the Pell equation which can be regarded as "$\mathbb{P}_1$ with many unit elements".
(2) By the same method $(*)$ above, we can find two Dirichlet L-functions which can be connected to $L(E, 1)$ with a higher order. If we assume that the Birch and Swinnerton-Dyer conjecture holds, one can say that the (non-torsion) rational points on an elliptic curve are all parametrized by the unit elements of $\mathcal{O}_K^*$ and $\mathcal{O}_L^*$ for some number fields K and L.

4. Comments on zeta elements

4.1. **Preliminary.**

4.1.1. *Numerical invariants.* An Euler system is a collection of classes in the Galois cohomology $H^1(K,-)$ which satisfies good Galois equivariant properties. Since its functoriality describes the local factors of L-functions, one can say that an Euler system is closely related to numerical (or local) invariants such as the number of $\mathbb{F}_p$-valued points,...et al.

4.1.2. *Geometric invariants.* (See [M1]) Let U be a smooth and separated scheme of finite type over $\mathbb{C}$ and X be a smooth compactification of U such that $D = X\backslash U$ is a globally normal crossing divisor. Then, by using the z-structure and ω-structure, one can investigate whether a cycle exists on schemes and how a cycle intersects with other cycles. Imitating the concept of Euler systems, let us consider $\mathrm{Ext}^1_{\mathrm{GMHS}}(\mathbb{Q}_M,-)$. Gathering a good collection of classes in this extension group, one may deduce geometric (or global) invariants of L-functions such as periods, regulators,...et al.

4.2. **Refinements.** Let X be a smooth proper scheme over $\mathbb{Q}$. Then, we have the étale cohomology group $H_{\text{ét}}(X\times\overline{\mathbb{Q}},\mathbb{Q}_l)$ equipped with the continuous action of $G=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On the other hand, let GS denote the analogous category of GMHS whose objects are $\mathbb{Q}_l$-vector spaces equipped with the z-structure and ω-structure and morphisms are given in an evident way. By using the z-structure and ω-structure with respect to X, $H_{\text{ét}}(X,\mathbb{Q}_l)$ can be regarded as an object of GS. Then, we have a natural morphism of $\mathbb{Q}_l$-vector spaces

$$\mathrm{Ext}^1_{\mathrm{GS}}(\mathbb{Q}_{l,M},H_{\text{ét}}(X,\mathbb{Q}_l))\to\mathrm{Ext}^1_{\mathrm{GS}}(\mathbb{Q}_{l,M},H^1(G,H_{\text{ét}}(\overline{X},\mathbb{Q}_l)))$$

where $\mathbb{Q}_{l,M}$ is a one dimensional $\mathbb{Q}_l$-vector space equipped with the z-structure and ω-structure with respect to X. One can say that a good collection of classes in $\mathrm{Ext}^1_{\mathrm{GS}}(\mathbb{Q}_{l,M},H^1(G,H_{\text{ét}}(\overline{X},\mathbb{Q}_l)))$ would connect the numerical (or local) invariants with the geometric (or global) invariants and would be a good candidate of zeta elements. Furthermore, let Y (resp. Z) be a smooth proper scheme over $\mathbb{Q}$ and c_Y (resp. c_Z) denote such a good element in the extension group above. Then, the elements

$$tc_Y+(1-t)c_Z\quad(0\le t\le 1)$$

have good functorial properties which are deduced from those of c_Y and c_Z and know the topological aspects of numerical and geometric invariants.

References

[CW] Coates, J.; Wiles, A.:*On the conjecture of Birch and Swinnerton-Dyer.* Invent. Math. 39 (1977), no. 3, 223–251.

[GZ] Gross, B.H.; Zagier, D.B.:*Heegner points and derivatives of L-series.* Invent. Math. 84 (1986), no. 2, 225–320.

[Ka] Kato, K.:*p-adic Hodge theory and values of zeta functions of modular forms.* Cohomologies p-adiques et applications arithmetiques. III. Astérisque No. 295 (2004), 117–290.
[Ko] Kolyvagin, V.A.:*Finiteness of* $E(\mathbb{Q})$ *and* Ш $(E, \mathbb{Q})$ *for a subclass of Weil curves.* Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671.
[M1] Morita, K.:*Generalization of the theory of mixed Hodge structures and its application.*
[M2] Morita, K.:*On the topological aspects of arithmetic elliptic curves.*
[M3] Morita, K.:*Deformation theory of quantum fields.* In Japanese.
[TW] Taylor, R.; Wiles, A.:*Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553–572.
[Wi] Wiles, A.:*Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443–551.

Department of Mathematics, Hokkaido University, Sapporo 060-0810, Japan

E-mail address: morita@math.sci.hokudai.ac.jp