Exposé court

52 *On the elliptic Gauss sums*

Goto, Akihiro (Kyushu university)

We denote K imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. The elliptic Gauss sum introduced by Asai is an analogous object to an elliptic curve (with CM by K) of the classical Gauss sum. For example, the classical Gauss sum appears as the value of the Dirichlet L-function at $s=1$, but Asai has shown that the elliptic Gauss sum appears as the value of the Hasse–Weil L-function at $s=1$ for CM elliptic curves.

There is also a congruence formula which is known by Cauchy between the class number of an imaginary quadratic field and the Bernoulli numbers. For an infinite family of elliptic curves $\{E_\lambda/K\}$ with CM by K as an analogue of the congruence, we obtain a congruence between the order of the Tate–Shafarevich group of E_λ/K and the Bernoulli–Hurwitz type number by using the elliptic Gauss sum. Here, λ is degree 1 prime element of K. This requires the assumption that the elliptic Gauss sum does not vanish, i.e., the value of the Hasse–Weil L-function at $s=1$ does not vanish. The Bernoulli–Hurwitz numbers are obtained as expansion coefficients of some elliptic functions.

In addition, we obtained that vanishing the elliptic Gauss sum is equivalent to that a certain Bernoulli–Hurwitz type number is divisible by ℓ which is norm prime of λ. This fact can be proved by viewing the elliptic Gauss sum as an element of a local field and using the theory of Lubin–Tate formal group. Using these conditions, we know that if the Hasse–Weil L-function of a CM elliptic curve at $s=1$ does not vanish, then the order of its Tate–Shafarevich group is not divisible by ℓ. In this presentation, I will summarize these facts.