Research summary

Tadahisa Nara

An elliptic curve is an algebraic curve E defined by a cubic equation called a Weierstrass equation. It is known that elliptic curves have a group structure, where the point at infinity O is the identity element. The set of rational points of E denoted by $E(\mathbb{Q})$ is known to be a finitely generated abelian group (Mordell–Weil group). Mordell–Weil groups of elliptic curves have been studied for a long time.

Duquesne and Fujita considered the elliptic curve defined by the equation $y^2 = x^3 - nx$, where n has a certain form (the curve has explicit rational points). They showed not only that the points are independent but also that the points always can be a part of the free part of the Mordell–Weil group of the curve ([1],[2]).

In a joint study with Fujita I considerd the elliptic curve defined by the equation $y^2 = x^3 + n$, where n has a certain form and we showed a similar result for the curve.

Our proof is along similar line to Duquesne's, that is, we estimated the values of the canonical heights and applied Siksek's theorem. The estimates were done by using the decomposition of the canonical height into local heights. Further we computed the local heights by using Tate's formula, Cohen's formula and Silverman's algorithm appropriately. In a process of the proof we needed upper bounds of the explicit points. The bounds was small enough in the case of Duquesne's. But in our case the bounds were not so small and we supplemented the gap with an argument of descent.

Siksek's theorem we mentioned above comes from the theory of quadratic forms. This theorem gives a lower bound of the regulator of an elliptic curve from a lower bound of the canonical height. (Precisely we need multiply it by a certain constant with respect to the rank.) That enable us to know how far the set of the points we choose is from a basis.

In addition I considered quadratic twists of elliptic curves in a similar direction([B]). In this case we also need a lower bound of the canonical height. I gave a lower bound by making use of an identity between division polynomials of elliptic curves. As an application of it, for a family of elliptic curves which I constructed, I showed that an explicit rational point is primitive.

References

[1] S. Duquesne. Elliptic curves associated with simplest quartic fields. *J. Theor. Nombres Bordeaux*, Vol. 19, pp. 81–100, 2007.

[2] Y. Fujita and N. Terai. Generators for the elliptic curve $y^2 = x^3 - nx$. *J. Theor. Nombres Bordeaux*, Vol. 23, pp. 403–416, 2011.