FAMILIES OF ELLIPTIC CURVES WITH PRESCRIBED TORSION

DAEYEOL JEON (JOINT WORK WITH YOONJIN LEE AND CHANG HEON KIM)

Abstract. In this talk, we construct some families of elliptic curves with prescribed torsion subgroups over quadratic and cubic number fields.

Mazur [Ma] proved that the torsion group \( E(\mathbb{Q})_{\text{tors}} \) of an elliptic curve \( E \) over the rational numbers must be isomorphic to one of the following 15 types:

\[
\mathbb{Z}/N\mathbb{Z}, \quad N = 1 - 10, 12 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, \quad N' = 1 - 4.
\]

Actually, each of these group occurs infinitely often as \( E(\mathbb{Q})_{\text{tors}} \). (By infinitely often in this context we always mean for infinitely many absolutely non-isomorphic \( E \), or in other words, for infinitely many different \( j \)-invariants \( j(E) \).) This is mainly due to the fact that the modular curves parametrizing elliptic curves with such a torsion structure are rational and hence have infinitely many \( \mathbb{Q} \)-rational points. In fact, Kubert [Ku] construct some families of elliptic curves with the torsion subgroup which contains such a group structure.

If \( E \) is an elliptic curve over a quadratic number field \( K \), then \( E(K)_{\text{tors}} \) must be isomorphic to one of the following groups which is described by Kamienny and Mazur [K-M]:

\[
\mathbb{Z}/N\mathbb{Z}, \quad N = 1 - 16, 18 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, \quad N' = 1 - 6 \\
\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N''\mathbb{Z}, \quad N'' = 1 - 2 \\
\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\]

Again, each of these 26 groups occurs infinitely often as \( E(K)_{\text{tors}} \), provided we allow the quadratic field \( K \) to vary too. It means that we can construct some families of elliptic curves with the torsion subgroup which
contains such a group structure. The main reason for this is that the modular curves which parametrize these torsion structures are rational, elliptic or hyperelliptic, and hence have infinitely many points that are rational or quadratic over \( \mathbb{Q} \).

Based on this observation, the author with Kim and Schweizer [J-K-S] proved that if \( K \) varies over all cubic number fields and \( E \) varies over all elliptic curves over \( K \), the group structures which appear infinitely often as torsion groups \( E(K)_{\text{tors}} \) are exactly the following:

\[
\mathbb{Z}/N\mathbb{Z}, \quad N = 1 - 16, 18, 20 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, \quad N' = 1 - 7.
\]

In this case we can also expect to construct some families of elliptic curves with the torsion subgroup which contains such a group structure. In our proof the main step was the classification of the modular curves parametrizing elliptic curves with such a torsion structure which have infinitely many cubic points, which turns out to be determination of the trigonal modular curves.

In this talk, we construct some families of elliptic curves with prescribed torsion subgroups over quadratic and cubic number fields.

**References**


Daeyeol Jeon, Department of Mathematics education, Kongju National University, 182 Shinkwan-dong, Kongju, Chungnam 314-701, Korea

E-mail address: dyjeon@kongju.ac.kr