CORENTIN PERRET-GENTIL, Centre de Recherches Mathématiques
Quotients of elliptic curves over finite fields

In fixed characteristic $p > 0$, there are only finitely many supersingular elliptic curves. Given a finite subgroup of such a curve, we can form the quotient, which is still a supersingular elliptic curve, isogenous to the base curve. For a family of subgroups of growing size (for example all cyclic subgroups of given cardinality), we would like to know how these quotients distribute in the isomorphism classes of supersingular elliptic curves. This question is related to the study of the security of recent cryptographic schemes using isogenies. The techniques involve applying the Riemann hypothesis over finite fields (in a general version) to exponential sums having high degree or to Jacobians of modular curves. Similar questions can be addressed for ordinary curves.