

Title: Point counting on reductions of CM elliptic curves.

Abstract: We give formulas for the number of points on an elliptic curve E over a finite field, when E is the reduction of an elliptic curve with complex multiplication. This is joint work with Karl Rubin, and generalizes to arbitrary CM elliptic curves earlier results of Dick Gross, Harold Stark, and others. An application is a simplification of the last step of the CM method for constructing an elliptic curve over a finite field with a specified number of points.