

1035-11-729

Alice Silverberg* (asilverb@math.uci.edu), Mathematics Department, UCI, 103 MSTB,
Irvine, CA 92697-3875. *Using complex multiplication to count points on elliptic curves.*

We give an explicit formula 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. As an application, we give an easy way to distinguish between the twists of E over \mathbb{F}_p in order to identify one with $p + 1 - 2U$ points, when $p = U^2 + dV^2$ with half-integers U and V and E is constructed using the CM method. This is joint work with K. Rubin, and extends to arbitrary CM elliptic curves earlier results of B. Gross and H. Stark who considered the case of CM by the ring of integers in $\mathbb{Q}(\sqrt{-d})$ when d is squarefree and $3 \pmod{4}$ but not divisible by 3. (Received September 14, 2007)