MR0272786 (42 #7667) 14.40

Manin, Ju. I.

The p-torsion of elliptic curves is uniformly bounded. (Russian)

Izv. Akad. Nauk SSSR Ser. Mat. **33** 1969 459–465

This paper is a very important contribution to the arithmetic on elliptic curves. Let X be an elliptic curve defined over the field of complex numbers C. Let D be a cyclic subgroup of X of order p^m. The absolute invariants $j(X)$ and $j(X/D)$ are connected by the modular equation of level $p^m F_m[j(X), j(X/D)] = 0$. Let K be a number field. The above correspondence commutes with the action of $\mathrm{Gal}(\overline{K}/K)$.

The author shows that for large values of m the curve $F_m(X, Y) = 0$ contains a finite number of K-rational points.

This plus the fact that the torsion of curves with fixed invariant $j \in K$ is bounded [V. A. Dem′janenko, Mat. Zametki **3** (1968), 271–278; MR0227166 (37 #2751)] gives the main result of the paper: If K is a number field, then there exists a constant c such that the order of the p-torsion group of the K-rational points of an elliptic curve defined over K does not exceed c.

The proof of the finiteness of the number of K-rational points on $F_m(X, Y) = 0$ is based on the following result: Let X ($X(K)$, $A(K)$ denote sets of K-rational points on X and A, respectively) be a curve and A a K-simple abelian variety contained in the jacobian of X with multiplicity $m(X, A)$ (to within isogeny). If $m(X, A) > \mathrm{rk}\, A(k)/\mathrm{rk}\, \mathrm{End}_k A$, then the set $X(K)$ is finite.

The above is obtained as a corollary to the following important theorem proved in this paper: Let $A(X)$ be the group of K-homomorphisms of a normal projective variety X into an abelian variety A taking a fixed point $x \in X(K)$ into zero. Assume that the rank of the Néron-Severi group of X is 1. If $\mathrm{rk}\, A(X) > \mathrm{rk}\, A(K)$, then the set $X(K)$ is finite.

The author also proves the following: Let X be an elliptic curve over k that has no complex multiplication. Then on the set of its K-forms the order of a maximal cyclic p-subgroup rational over K is bounded.

Reviewed by *J. Blass*