HOW MANY RATIONAL POINTS ARE THERE AND ARE THERE ALGORITHMS TO FIND THEM?

BARRY MAZUR

1. Diophantine Stability and Hilbert's Tenth Problem

A variety V over a field K is **Diophantine Stable** (**DS**) relative to (or "for") the field extension L/K if V "acquires no new points" when you extend its base to L. I.e., if:

$$V(K) = V(L).$$

Karl Rubin and I proved that if A is a simple abelian variety over K and all $\bar{K}$-endomorphisms of A are defined over K there are infinitely many (Galois cyclic) extensions of K for which A is **DS**. We conjecture, in fact, that for any abelian variety A over K the non-**DS** Galois cyclic extensions are very rare.

To be more specific, we prove, for any simple abelian variety A satisfying the above condition over a number field K, and for every positive integer n there is a set S of prime numbers ℓ of positive density such that for any prime power ℓ^n where $\ell \in S$ and n is any natural number, there are infinitely many Galois cyclic extensions L/K of degree ℓ^n for which A is **DS**.

["Infinitely many," however, does not even mean "of positive density among all Galos cyclic extensions of degree ℓ^n."]

In contrast, we conjecture that if—for example—$K/\mathbf{Q}$ is of odd degree—then for any abelian variety A over K there is a finite bound $D(A;K)$ such that for any prime number $p > D(A;K)$ there are *no* Galois cyclic extensions L/K of degree p for which A is **DS**. There are some quite celebrated counter-examples to boundedness if $K/\mathbf{Q}$ is of even degree.

Hilbert's Tenth Problem: As one of our projects this MSRI DCC semester, Sasha Shlapentokh (and Rubin and I) want to construct a **Diophantine definition of $\mathcal{O}_K$ in $\mathcal{O}_L$** given any abelian variety over K

- with infinitely many K-rational points and
- for which L/K is **DS**.