The Néron-Ogg-Shafarevich criterion

Ravi Fernando – `fernando@berkeley.edu`

February 17, 2016*

1 Introduction

History: proved by Ogg (1967) for elliptic curves; Shafarevich seems to have been aware of it too. Proved by Serre and Tate (1968) for abelian varieties, using Néron models; they named it.

Let K be a field with a discrete valuation v, ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{m}$, and residue field $\mathcal{O}_K/\mathfrak{m} = k$. (Assume for convenience that k is perfect with characteristic not 2 or 3.) We mostly care about the case where K is a local field, and I will often use notation suggesting this, but the result holds in somewhat more generality.

Since Néron-Ogg-Shafarevich will give us a connection between the reduction of an abelian variety A/K and the ramification of its associated Galois representations (namely: good reduction $\leftrightarrow$ unramified Galois representations), we will begin by defining these notions.

Choose a separable closure K^s of K and an extension $\overline{v}$ of v. This determines a decomposition group $D_{\overline{v}|v}$ and an inertia group $I(\overline{v}) = \ker(D_{\overline{v}|v} \to G_k) \leq \mathrm{Gal}(K^s/K) = G_K$. We will usually forget about $\overline{v}$ and write the inertia group as I_K because it is determined up to conjugacy in G_K by K and v. We say that a G_K-module is *unramified* if I_K acts trivially on it. (Motivation: a Galois extension L/K, equipped with the obvious G_K-action, is unramified if and only if it is unramified at v in the usual sense.)

Let A be an abelian variety over K. We would like to study the "reduction of A modulo $\mathfrak{m}$", but this doesn't (yet) make any sense: k isn't generally even a subfield of K. There are n ways to make this precise:

1. We say that A/K has *good reduction at v* if there exists an abelian scheme (smooth proper group scheme with geometrically connected fibers) A_v over $\mathcal{O}_v$ whose generic fiber $A_v \times_{\mathcal{O}_v} K$ is isomorphic (over K) to A. In particular, this requires the special fiber $A_v \times_{\mathcal{O}_v} k$ to be an abelian variety over k.

*Notes for a talk given in Berkeley's student arithmetic geometry seminar. Various references: Pietro Gatti's thesis, "The Néron-Ogg-Shafarevich Criterion"; Lecture 8-9 notes for Andrew Snowden's Math 679, "Elliptic curves over DVRs" and "Néron models"; Chapter VII of Silverman's *The arithmetic of elliptic curves*; Serre and Tate, "Good reduction of abelian varieties".

2. ϵ more concrete: Néron models. If the abelian scheme A_v above exists, it is the Néron model of A. So if we want to check whether A has good reduction, we could in principle compute the Néron model and see whether or not it's proper (and thus an abelian scheme). The problem is that Néron models are very difficult to compute in general, and not easy even in the elliptic curve case.

3. Elliptic curve case: easy to check by minimal Weierstrass models. (These are different from Néron models though.)

4. A somewhat counterintuitive fact: there is actually a "reduction map" from A/K to its reduction $\widetilde{A}/k$. An ugly description: given a K-point of A, write down the projective coordinates $[x_0; \cdots ; x_N]$, scale so that they are all integral and not all in $\mathfrak{m}$, and literally reduce mod $\mathfrak{m}$. This obviously can't be made into a morphism of schemes in general (think mixed characteristic), but we will later see that Néron models give us a nice, natural way to reinterpret this.

2 Reduction of elliptic curves

Let $A = E$ be an elliptic curve over K. We can write down a Weierstrass model $y^2 = x^3 + ax + b$ (if $\operatorname{char} K \neq 2, 3$), where $a, b \in K$ and the discriminant $\Delta = -16(4a^3 + 27b^2)$ is nonzero. Notice that this isn't unique: if we multiply the equation by u^6 and substitute $y' = u^3 y$ and $x' = u^2 x$, then we get a new equation where a is multiplied by u^4 and b by u^6. (Thus Δ gets scaled by u^{12}.) Choosing appropriate values of u, we can ensure that $a, b \in \mathcal{O}_K$. Moreover, if we choose them to have the smallest possible nonnegative valuations, then this is a *minimal Weierstrass model*.

In the elliptic curve case, minimal Weierstrass models completely determine whether E has good reduction. Namely, if the discriminant Δ of the minimal Weierstrass model is nonzero mod $\mathfrak{m}$, then E has good reduction, and its reduction is defined by the same equation. If $a, b \neq 0$ but $\Delta = 0$, then E has multiplicative (nodal) reduction. If $a = b = 0$, then E has additive (cuspidal) reduction.

Elliptic curve case: good (reduction is an elliptic curve), multiplicative (reduction is nodal), additive (reduction has a cusp). This classification comes from writing down a minimal Weierstrass model $y^2 = x^3 + ax + b$ and studying a, b modulo $\mathfrak{p}$. (Modify this a little if $\operatorname{char} k = 2$ or 3.) "Semistable" means either good or multiplicative.

3 Néron models

Suppose we have an abelian variety over K, not necessarily with good reduction, and we want to extend it to a scheme over $\mathcal{O}_K$. There are potentially many ways to do this, but (at least in one sense) the "best" way is the Néron model. The Néron model A_v represents the following functor on the category of smooth separated $\mathcal{O}_K$-schemes Y:

$$\operatorname{Hom}(Y, A_v) = \operatorname{Hom}(Y \times_{\mathcal{O}_K} K, A) \tag{1}$$

(Draw some pictures here: the left-to-right map is restricting to the generic fiber, and the right-to-left map is the "Néron mapping property" that we can extend back up uniquely.) This of course determines A_v up to unique isomorphism if it exists, and in fact Néron proved that it does.

Basic facts about the Néron model: it is always smooth, but not necessarily proper. In fact, it is proper if and only if its special fiber is proper, which happens if and only if A has good reduction. It is always a group scheme, which we can see from its universal property: the group law on A becomes one on A_v. It is not obvious how to compute the Néron model in practice; in particular, even in the elliptic curve case; it isn't necessarily just the minimal Weierstrass model with the singularities removed. However, in the elliptic curve case, Tate's algorithm gives an 11-step process to determine what type of singular fiber it has.

4 Néron-Ogg-Shafarevich and a proof sketch

Let m denote an integer prime to $\mathrm{char}(k)$, and ℓ a prime not equal to $\mathrm{char}(k)$. Then we can consider the m-torsion $A[m] \cong (\mathbb{Z}/m)^{2\dim(A)}$, and the ℓ-adic Tate module $T_\ell A = \lim_{\leftarrow n} A[\ell^n] \cong \mathbb{Z}_\ell^{2\dim(A)}$. These are both G_K-modules. We claim that the Galois action on these modules contains the information of whether A has good or bad reduction at $\mathfrak{m}$.

Theorem 4.1. *The following are equivalent:*

(a) A has good reduction at $\mathfrak{m}$.

(b) The m-torsion $A[m]$ is unramified for all $m \geq 1$ relatively prime to $\mathrm{char}(k)$.

(c) The Tate module $T_\ell(A)$ is unramified for some ($\Leftrightarrow$ all) primes $\ell \neq \mathrm{char}(k)$.

(d) The m-torsion $A[m]$ is unramified for infinitely many $m \geq 1$ relatively prime to $\mathrm{char}(k)$.

Proof. The implications (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are clear by choosing $m = \ell^n$ and observing that $T_\ell A$ is unramified if and only if all $A[\ell^n]$ are unramified. So it will suffice to prove (a) $\Rightarrow$ (b) and (d) $\Rightarrow$ (a). (It is not a priori clear that (c) is independent of the choice of ℓ, but this follows from the theorem.)

Following the argument of Serre-Tate, we will now prove some lemmas that are useful for both (a) $\Rightarrow$ (b) and (d) $\Rightarrow$ (a). Fix $m \geq 1$ relatively prime to $\mathrm{char}(k)$.

Consider the special fiber $\widetilde{A}/k$ of the Néron model. This may be disconnected, but by Chevalley's structure theorem (since k is perfect), the connected component $\widetilde{A}^0$ fits into a short exact sequence $0 \to H \to \widetilde{A}^0 \to B \to 0$, where H is a linear algebraic group and B is an abelian variety. Moreover, H is the product of a torus $S \cong (\mathbb{G}_m)^d$ and a unipotent group U.

Lemma 4.2. *Let c be the index of $\widetilde{A}^0$ in $\widetilde{A}$, i.e. the number of components of $\widetilde{A}$. The $\mathbb{Z}/m\mathbb{Z}$-module $\widetilde{A}[m]$ is an extension of a group whose order divides c by a free $\mathbb{Z}/m\mathbb{Z}$-module of rank* $\dim(S) + 2\dim(B)$.

Proof. Take m-torsion of the short exact sequence above to get $0 \to H[m] \to \widetilde{A}^0[m] \to B[m] \to 0$; this is still exact because $H(\bar{k})$ is m-divisible. But $H[m] = S[m] = (\mathbb{G}_m)^{\dim S}[m] \cong \mu_m^{\dim S}$, and $B[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2\dim B}$, so the $\mathbb{Z}/m\mathbb{Z}$-module $\widetilde{A}^0[m]$ must be free of rank $\dim(S)+2\dim(B)$. But $\widetilde{A}^0[m]$ is normal in $\widetilde{A}[m]$, of index dividing $[\widetilde{A} : \widetilde{A}^0] = c$, so we have our extension. □

Now let $A[m]^I$ denote the set of m-torsion points of A fixed by the inertia group $I = I_K = I(\bar{v})$.

Lemma 4.3. *The reduction map defines an isomorphism $A[m]^I \to \widetilde{A}[m]$, which commutes with the action of the decomposition group.*

Proof. First we should say what the reduction map is, since we already discussed the fact that there is not in general any map of schemes $A \to \widetilde{A}$. There is actually a natural way to turn a K-point of A into a k-point of $\widetilde{A}$. Namely, the Néron mapping property says that $A(K)$ is in natural bijection with $A_v(\mathcal{O}_K)$, and this in turn maps to $\widetilde{A}(k)$ by restricting to the special fiber.

Let L be the fixed field of I_K, which (in the local field case) is the maximal unramified extension of K. Then by definition we have $\widetilde{A}[m] = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \widetilde{A}(\bar{k}))$ and

$$A[m]^I = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A(K^s))^I \tag{2}$$
$$= \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A(L)) \tag{3}$$
$$= \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A_v(\mathcal{O}_L)) \tag{4}$$

Here we are using the fact that $A_v \times_{\mathcal{O}_K} \mathcal{O}_L$ is a Néron model of A_L. So the reduction map here sends $A(L) = A_v(\mathcal{O}_L)$ to $\widetilde{A}(\mathfrak{l}) = \widetilde{A}(\bar{k})$. One can check that r is surjective and its kernel is uniquely m-divisible, which is enough to imply that it yields an isomorphism

$$A[m]^I = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A(L)) \to \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \widetilde{A}(\bar{k})) = \widetilde{A}[m] \tag{5}$$

□

We are now ready to prove (a) ⇒ (b). We are given A has good reduction. Then $\widetilde{A} = B$ is actually an abelian variety (whose dimension equals that of A), so $\widetilde{A}[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2\dim(\widetilde{A}) = 2\dim A$. By Lemma 4.3, $A[m]^I$ is isomorphic to it. But by order considerations, this means that $A[m]^I$ must be all of $A[m]$, so we are done.

Now let's prove (d) ⇒ (a). Here, we are given that there exist infinitely many integers m, coprime to $\mathrm{char}(k)$, such that $A[m]$ is unramified. Choose one such m that is greater than $c = [\widetilde{A} : \widetilde{A}^0]$. Then Lemma 4.2 gives us the inequality $m^{\dim(S)+2\dim(B)} \leq |\widetilde{A}[m]| \leq cm^{\dim(S)+2\dim(B)} < m^{\dim(S)+2\dim(B)+1}$. But by Lemma 4.3, $|\widetilde{A}[m]| = |A[m]^I| = |A[m]| = m^{2\dim(A)}$. It follows that $\dim(S) + 2\dim(B) = 2\dim(A) = 2(\dim(S) + \dim(B) + \dim(U))$. In particular, S and U are both trivial, so $\widetilde{A}^0 = B$. Thus the special fiber of the Néron model is proper. One can show that this implies the entire Néron model is proper, so A has good reduction, as claimed.

We've shown that (a) ⇒ (b) ⇒ (c) ⇒ (d) ⇒ (a), so we are done. □

5 Corollaries

5.1 Potential good reduction

Corollary 5.1. *An abelian variety A/K has potential good reduction (i.e. good reduction after a finite field extension) if and only if I_K acts via a finite quotient.*

5.2 Good reduction and isogenies

Corollary 5.2. *Let A_1 and A_2 be isogenous abelian varieties over K. Then A_1 has good reduction if and only if A_2 does.*

Proof. Suppose there is an isogeny $\phi : A_1 \to A_2$ of degree d. Choose a prime ℓ that doesn't divide d or $\mathrm{char}(k)$. Then ϕ induces an isomorphism of ℓ-adic Tate modules $T_\ell A_1 \to T_\ell A_2$, as G_K-modules. (The order of the kernel has to divide d but be a power of ℓ.) But good reduction can be detected on $T_\ell A$ for any $\ell \neq \mathrm{char}(k)$, so we are done. □