MAZUR'S EISENSTEIN DESCENT

JAMES PARSON

1. Introduction

The purpose of these notes is to illustrate the descent technique used in [Maz72] and [Maz77] to bound the rank of abelian varieties $A_{/\mathbf{Q}}$; this method is used in [Maz77] to prove that the Eisenstein quotient of $J_0(N)_{/\mathbf{Q}}$ (where N is a prime number) has rank 0. We begin with a brief review of the standard method of descent. We then explain how *fppf* cohomology can be used following this model to prove our main result (Theorem 3.1); an easy corollary is that an elliptic curve $E_{/\mathbf{Q}}$ has rank 0, if it has a non-zero torsion point of order prime to N, good reduction outside a prime N, and multiplicative reduction at N. Finally, the last two sections of the notes provide some examples of abelian varieties to which the theorem applies, constructed using Tate normal form and modular curves.

2. Review of Descent

Before we get to Mazur's methods, let us review the classical descent procedure in cohomological terms, following [Sil86], Chapter X. Let $A_{/K}$ be an abelian variety, where K is a number field, and let n be a non-zero rational integer. One has the following exact sequence over K (of algebraic groups, group schemes, étale sheaves, *fppf* sheaves, *etc.*):

$$0 \to A[n] \to A \xrightarrow{n} A \to 0.$$

From this short exact sequence, one derives the long exact sequence in Galois cohomology, out of which one extracts

$$0 \to A(K)/nA(K) \to \mathrm{H}^1(K, A[n]) \to \mathrm{H}^1(K, A)[n] \to 0. \tag{1}$$

This sequence is not immediately useful because the two cohomology groups that appear are infinite. One observes, however, that one may replace these cohomology groups with subgroups determined by certain local conditions: for any place v of K, one can consider the restriction map $\mathrm{H}^1(K, A[n]) \to \mathrm{H}^1(K_v, A[n])$. One has the local analogue of (1) for each place v of K:

$$0 \to A(K_v)/nA(K_v) \to \mathrm{H}^1(K_v, A[n]) \to \mathrm{H}^1(K_v, A)[n] \to 0. \tag{2}$$

Write L_v for the image of $A(K_v)/nA(K_v)$ in $\mathrm{H}^1(K_v, A[n])$. The subgroup of classes in $\mathrm{H}^1(K, A[n])$ that restrict to elements of L_v for each v is called the *n-Selmer group*, $\mathrm{Sel}^{(n)}(A/K)$. Evidently the image of $A(K)/nA(K)$ lands in $\mathrm{Sel}^{(n)}(A/K)$, since restriction maps are compatible with coboundary maps.

To prove the weak Mordell-Weil theorem (*viz* that $A(K)/nA(K)$ is finite) it remains only to show that $\mathrm{Sel}^{(n)}(A/K)$ is finite. The key to this finiteness is that for any finite place v of K that is prime to n and where A has good reduction, the subgroup $L_v \subset H^1(K_v, A[n])$ is precisely the subgroup of all *unramified* cohomology classes. (Recall that for a local Galois module M, a class in $\mathrm{H}^1(K_v, M)$ is *unramified*, if it is split by an unramified extension of K_v.) It is a general fact in Galois cohomology that if M is a discrete, finite $\mathrm{Gal}(\overline{K}/K)$-module, then the subgroup of classes in $\mathrm{H}^1(K, M)$ that are unramified outside a fixed finite set of places S is finite.

Having refined the middle term of (1), we turn to the rightmost term: consider $\mathrm{H}^1(K, A)$. The subgroup $Ш(A/K)$ of classes that restrict to the identity in $\mathrm{H}^1(K_v, A)$ for all places v of K is called the *Tate-Shafarevich group*. If v is a finite place where A/K has good reduction, then the identity is the only unramified class in $\mathrm{H}^1(K_v, A)$. Note, however, that the general finiteness fact used above to show that $\mathrm{Sel}^{(n)}(A/K)$ is finite does not apply to $Ш(A/K)$; nonetheless, it is conjectured to be a finite group. The exact sequences (1) and

(2) show that the image of $\mathrm{Sel}^{(n)}(A/K)$ in $\mathrm{H}^1(K,A)$ is precisely $Ш(A/K)[n]$, which is therefore finite. We now have the refined n-descent exact sequence

$$0 \to A(K)/nA(K) \to \mathrm{Sel}^{(n)}(A/K) \to Ш(A/K)[n] \to 0, \tag{3}$$

in which all three terms are known to be finite. It is possible to compute $\mathrm{Sel}^{(n)}(A/K)$, but one cannot easily determine if a given class in the Selmer group maps to 0 in $Ш(A/K)[n]$. The general method to answer such a question involves iterating the descent procedure ("second descent," *etc.*).

2.1. **A simple bound on the rank.** Here is a simple example of how the theoretical considerations above can be used to get a bound on ranks. Let $E_{/K}$ be an elliptic curve and suppose that $E(K)$ contains the full 2-torsion. Then as group schemes (or as Galois modules)

$$E[2] = \underline{\mathbf{Z}/2\mathbf{Z}} \times \underline{\mathbf{Z}/2\mathbf{Z}} = \mu_2 \times \mu_2;$$

consequently, we have

$$\mathrm{H}^1(K, E[2]) = K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Let S be a finite set of places of K containing the infinite places, places over 2, and the places of bad reduction for E. Then $\mathrm{Sel}^{(2)}(E/K)$ is contained in the group of classes in $\mathrm{H}^1(K, E[2])$ that are unramified outside of S. Explicitly, this is a sum of two copies of $K(S,2)$, the group of all classes in $K^\times/(K^\times)^2$ with even valuation at places outside S. In particular, if $K = \mathbf{Q}$, then the order of $\mathrm{Sel}^{(2)}(E/\mathbf{Q})$ is bounded by $2^{2\#S}$; since $E(\mathbf{Q})/2E(\mathbf{Q})$ injects into the Selmer group, we conclude that the rank ρ of $E_{/\mathbf{Q}}$ is bounded by $2\#S - 2$. Note that in producing this upper bound on the rank, we threw away all information at ramified primes (*viz* $2, \infty$, and the primes of bad reduction).

Mazur's bounds in [Maz72] and [Maz77] are similar in spirit but use *fppf* cohomology to get better estimates on the order of Selmer groups. For instance, if one applied the above Galois-cohomology bound to an elliptic curve $E_{/\mathbf{Q}}$ with prime conductor $N \neq 2$ and full 2-torsion in $E(\mathbf{Q})$, then one would get $\rho \leq 4$; Mazur's method yields $\rho = 0$.

2.2. **Reformulation using étale cohomology.** In order to make the relation between Mazur's bounds and the classical descent as clear as possible, let us recast some of the classical picture in terms of étale cohomology. Consider an abelian variety $A_{/\mathbf{Q}}$ and let $\mathcal{A}$ be its Néron model over $\mathbf{Z}$. We will study p-descent on A for p a prime. Choose $N \in \mathbf{Z}$ so that A has good reduction outside of primes dividing N and so that $p|N$. Then $\mathcal{A}_{/\mathbf{Z}[1/N]}$ is an abelian scheme and $[p] : \mathcal{A} \to \mathcal{A}$ is étale (and surjective) over $\mathbf{Z}[1/N]$. Consequently, we have an exact sequence of étale sheaves on $\mathrm{Spec}(\mathbf{Z}[1/N])$:

$$0 \to \mathcal{A}[p] \to \mathcal{A} \xrightarrow{p} \mathcal{A} \to 0.$$

From the long exact cohomology sequence, one extracts

$$0 \to \mathcal{A}(\mathbf{Z}[1/N])/p\mathcal{A}(\mathbf{Z}[1/N]) \to \mathrm{H}^1_{\text{ét}}(\mathbf{Z}[1/N], \mathcal{A}[p]) \to \mathrm{H}^1_{\text{ét}}(\mathbf{Z}[1/N], \mathcal{A})[p] \to 0.$$

The first term is simply $A(\mathbf{Q})/pA(\mathbf{Q})$ by the Néron mapping property. The second and third terms can be interpreted classically: $\mathrm{H}^1_{\text{ét}}(\mathbf{Z}[1/N], \mathcal{A}[p])$ is naturally the group of classes in $\mathrm{H}^1(\mathbf{Q}, A[p])$ that are unramified away from N and ∞; similarly $\mathrm{H}^1_{\text{ét}}(\mathbf{Z}[1/N], \mathcal{A})$ consists of classes in $\mathrm{H}^1(\mathbf{Q}, A)$ that are unramified (and hence split) away from N and ∞. Concretely, this exact sequence from étale cohomology yields upper bounds on the Selmer group by imposing the condition "unramified" on classes at the primes not dividing N and no conditions at infinity and at primes dividing N. Mazur's approach is to replace the étale cohomology over $\mathbf{Z}[1/N]$ with *fppf* cohomology over $\mathbf{Z}$, imposing conditions at all finite places to obtain a better estimate on the size of the Selmer group.

3. Mazur's *fppf* descent

In this section, we give a typical example of using the *fppf* site on $\mathrm{Spec}(\mathbf{Z})$ to bound ranks. The theorem below is adapted for application to the Eisenstein quotients of modular Jacobians; refinements for elliptic curves can be found in §9 of [Maz72]. The notation and terminology below follow §I.1 of [Maz77]. Fix a prime number N and a second, distinct prime p. Here is the main result:

Theorem 3.1. *Let $A_{/\mathbf{Q}}$ be an abelian variety with good reduction outside of N and purely toric reduction at N. Suppose moreover that $\mathcal{A}[p]$ is admissible, where $\mathcal{A}_{/\mathbf{Z}}$ is the Néron model. Then $A_{/\mathbf{Q}}$ has rank 0.*

For the definition of *admissible*, see §I.1 of [Maz77]. Before we start the proof, note that the hypotheses and the conclusion depend only on $A_{/\mathbf{Q}}$ up to $\mathbf{Q}$-isogeny. For admissibility, one can use the Brauer-Nesbitt theorem, which shows that the factors in a composition series of the Galois module $A[p](\overline{\mathbf{Q}})$ depend only on the Galois representation on $V_p(A/\mathbf{Q})$ and hence only on $A_{/\mathbf{Q}}$ up to isogeny. One can find the isogeny properties of the two hypotheses on the reduction of $A_{/\mathbf{Q}}$ in [BLR90].

Proof. Before we begin to study A, let us replace it with $A \times A^\vee$. It suffices, of course, to prove that the rank of $(A \times A^\vee)(\mathbf{Q})$ is 0. Since the hypotheses of the theorem depend only on $A_{/\mathbf{Q}}$ up to isogeny, they are satisfied by $A^\vee_{/\mathbf{Q}}$ and hence also by $A \times A^\vee$ over $\mathbf{Q}$. The advantage of this adjustment is that we can assume that $\mathcal{A}[p]_{/\mathbf{Z}[1/N]}$ is its own Cartier dual, which is used below to compute α. There are several variants on this trick that one could use in its place.

Let $\mathcal{A}^0_{/\mathbf{Z}}$ be the (fiberwise) identity component of $\mathcal{A}_{/\mathbf{Z}}$, which is the open subgroup of $\mathcal{A}_{/\mathbf{Z}}$ obtained by removing the non-identity components of the fiber over (N). The semi-abelian reduction hypothesis ensures that the multiplication-by-p map $[p] : \mathcal{A}^0 \to \mathcal{A}^0$ is surjective (and flat by the "miracle flatness theorem"), and so we have the following exact sequence of *fppf* sheaves on $\mathrm{Spec}(\mathbf{Z})$:

$$0 \to \mathcal{A}^0[p] \to \mathcal{A}^0 \xrightarrow{p} \mathcal{A}^0 \to 0.$$

Passing to the long exact sequence in *fppf* cohomology over $\mathbf{Z}$, one extracts the short exact sequence

$$0 \to \mathcal{A}^0(\mathbf{Z})/p\mathcal{A}^0(\mathbf{Z}) \to \mathrm{H}^1_{\mathrm{fppf}}(\mathbf{Z}, \mathcal{A}^0[p]) \to \mathrm{H}^1_{\mathrm{fppf}}(\mathbf{Z}, \mathcal{A}^0)[p] \to 0.$$

As in [Maz77], let $h^i = \log_p \#\mathrm{H}^{\mathrm{i}}_{\mathrm{fppf}}(\mathbf{Z}, \mathcal{A}^0[\mathrm{p}])$. Note that $\mathcal{A}^0(\mathbf{Z})$ has finite index in $\mathcal{A}(\mathbf{Z}) = A(\mathbf{Q})$, and so $\mathcal{A}^0(\mathbf{Z})$ is isomorphic to $\mathbf{Z}^\rho \oplus T$, where ρ is the rank of $A_{/\mathbf{Q}}$ and T is a finite abelian group. Therefore, $\mathcal{A}^0(\mathbf{Z})/p\mathcal{A}^0(\mathbf{Z})$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{\rho+h^0}$; consequently, we have $\rho + h^0 \le h^1$, or, equivalently, $\rho \le h^1 - h^0$.

The group scheme $\mathcal{A}^0[p]$ is admissible by assumption, and so by [Maz77] Proposition 1.7, we have $h^1 - h^0 \le \delta - \alpha$, where δ (defect) and α (additive part) are as defined on page 47 of [Maz77]. These invariants are easy to compute: since $\mathcal{A}^0_{/\mathbf{F}_N}$ is a torus, $\mathcal{A}^0_{/\mathbf{F}_N}[p]$ has rank p^g, where $\dim(A) = g$, and so $\delta = 2g - g = g$. To evaluate α, it suffices to recall that $\mathcal{A}^0[p]_{/\mathbf{Z}[1/N]} = \mathcal{A}[p]_{/\mathbf{Z}[1/N]}$ is its own Cartier dual (because of the trick at the start of the proof); from this self-duality, it follows that the number of $\underline{\mathbf{Z}/p\mathbf{Z}}$'s in a composition series is the same as the number of μ_p's, and so (recalling admissibility) $\alpha = 2g/2 = g$. Consequently, we have $\rho \le \delta - \alpha = g - g = 0$, and the theorem is proved. □

We have the following immediate corollary of the theorem:

Corollary 3.2. *Let $E_{/\mathbf{Q}}$ be an elliptic curve with good reduction outside of N and multiplicative reduction at N. If $E_{/\mathbf{Q}}$ has a non-zero torsion point of order prime to N, then it has rank 0.*

Proof. Choose a prime $p \neq N$ so that $E_{/\mathbf{Q}}$ has a non-zero p-torsion point P. Then the Galois module $E[p](\overline{\mathbf{Q}})$ contains $\mathbf{Z}/p\mathbf{Z}$ as a sub-Galois module (with generator P). The Weil pairing identifies the quotient Galois module with μ_p, and so $\mathcal{E}[p]$ is admissible (see page 47 of [Maz77]). Now the theorem applies to show $E_{/\mathbf{Q}}$ has rank 0. Note, incidentally, that the trick at the beginning of the proof of the theorem is unnecessary in this case, since the scheme-theoretic Weil pairing identifies $\mathcal{E}[p]_{/\mathbf{Z}[1/N]}$ with its Cartier dual. For computing α, it suffices, in fact, to check the geometric fiber at p, where one can even use the standard Weil pairing discussed in [Mum70] to complete the argument. □

4. Tate-normal-form examples

Using the special forms for elliptic curves that Bryden and I discussed last term (and which are also used in [Kub76] and [Con95]), one can produce a few nice examples to which the corollary applies. My method for finding good parameters in the equations below was to find discriminants that match curves I know exist from the theory of modular Jacobians. (As I explained in my notes from last term, it is not too difficult to identify examples produced by this method with those coming from modular curves. Of course by fancy

theorems, one knows that such identifications can be made in general.) By the corollary, the following elliptic curves (presented in Weierstrass form) have rank 0 over $\mathbf{Q}$:

$$\begin{aligned} y^2 + 2xy + 19y &= x^3, & \Delta &= -19^3, & &\text{where } (0,0) \text{ is 3-torsion;} \\ y^2 + 10xy + 37y &= x^3, & \Delta &= 37^3, & &\text{where } (0,0) \text{ is 3-torsion;} \\ y^2 + xy - y &= x^3 - x^2, & \Delta &= 17, & &\text{where } (0,0) \text{ is 4-torsion;} \\ y^2 - y &= x^3 - x^2, & \Delta &= -11, & &\text{where } (0,0) \text{ is 5-torsion;} \\ y^2 - 10xy - 11y &= x^3 - 11x^2, & \Delta &= -11^5, & &\text{where } (0,0) \text{ is 5-torsion.} \end{aligned}$$

The results of [Maz72] apply to some cases of additive reduction and to some cases when there are several places of bad reduction; most of the examples of elliptic curves over $\mathbf{Q}$ with one or two places of bad reduction and non-zero torsion points can be checked readily to have rank 0 using the bounds there.

5. Modular-curves examples

This section applies Theorem 3.1 to factors of Jacobians of modular curves. As I discussed in my notes last term, there is a proper, smooth model of $X_0(N)$ over $\mathbf{Z}[1/N]$; one concludes from this, using the relative theory of Pic^0, that $J_0(N)_{/\mathbf{Q}}$ has good reduction away from N. Later this term, we will study the geometry of a modular model of $X_0(N)$ over $\mathbf{Z}$, which has singularities in its fiber over (N). One can analyze these singularities using modular techniques; the ultimate conclusion is that $J_0(N)_{/\mathbf{Q}}$ has purely toric reduction at N. (One can compute the component group and character group of the bad fiber as well.) Recall that in my notes from last term, I checked this fact directly for $J_0(11)_{/\mathbf{Q}}$ by finding an explicit Weierstrass equation (using Tate normal form and the cusps). In the following, I will analyze the torsion of quotients of $J_0(N)_{/\mathbf{Q}}$ following [Maz77].

5.1. **Three special cases.** Before turning to the general case, we consider three special cases, namely $J_0(N)_{/\mathbf{Q}}$ with $N = 11, 17, 19$. These are the three cases where $J_0(N)$ (for N prime) is an elliptic curve. (If one drops the condition that N be prime, one finds elliptic curves for $N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36,$ and 49.) By the above paragraph, we know that these $J_0(N)_{/\mathbf{Q}}$ have good reduction outside of N and multiplicative reduction at N. We produce a non-zero torsion point (of order prime to N) on each, which shows that they all have rank 0 over $\mathbf{Q}$.

Recall that $X_0(N)_{/\mathbf{Q}}$ has two cusps, both $\mathbf{Q}$-rational, usually called 0 and ∞. In modular terms, 0 is the N-gon cusp, and ∞ is the 1-gon cusp. We consider the point $c = [0] - [\infty] \in J_0(N)(\mathbf{Q})$. Since $X_0(N)$ does not have genus 0, we know $c \neq 0$. Furthermore, since $\Delta(q)/\Delta(q^N)$, which is a rational function on $X_0(N)_{/\mathbf{C}}$, has divisor $(N-1)([0]-[\infty])$, the point c has order dividing $N-1$. In particular, it is a non-zero torsion point of order prime to N on $J_0(N)_{/\mathbf{Q}}$. The existence of this torsion point allows us to apply the corollary and thus to conclude that $J_0(N)_{/\mathbf{Q}}$ has rank 0 for $N = 11, 17, 19$. (It is no accident, of course, that these N show up in the discriminants of the Tate-normal-form examples. The prime 37 occurs among those examples, since the Eisenstein quotient of the 2-dimensional $J_0(37)_{/\mathbf{Q}}$ is an elliptic curve.)

5.2. **The general case.** Now consider the general case of $J_0(N)_{/\mathbf{Q}}$ for a prime N such that $X_0(N)$ does not have genus 0. The analysis of the previous paragraph applies to show that $c = [0] - [\infty]$ is a non-zero (rational) torsion point of order dividing $N-1$. One can say a bit more about it: since the Atkin-Lehner involution w_N switches 0 and ∞, we have $w_N c = -c$. Furthermore, it is easy to see that for primes $l \neq N$, one has $T_l[0] = (l+1)[0]$ and $T_l[\infty] = (l+1)[\infty]$, and so $T_l c = (l+1)c$. Consequently, the Hecke algebra $\mathbf{T}$ (which is generated by the T_l and $w_N = -U_N$) acts on c via its Eisenstein quotient; indeed, the Eisenstein ideal of $\mathbf{T}$ is generated by the relations $w_N = -1$ and $T_l = l + 1$ for all primes $l \neq N$. Since c has order dividing $N-1$, we see that there is an Eisenstein prime ideal of $\mathbf{T}$, i.e. a prime ideal containing the Eisenstein ideal, with residue characteristic prime to N. (If one prefers, it is possible to construct such a prime ideal by the dual technique of analyzing the normalized Eisenstein series on $\Gamma_0(N)$.)

As Brian explained in his introductory lecture (using the Eichler-Shimura construction), the existence of such a prime ideal of $\mathbf{T}$ with residue characteristic $p \neq N$ implies the existence of a non-trivial isogeny

factor $A_{/\mathbf{Q}}$ of $J_0(N)_{/\mathbf{Q}}$ such that $\mathcal{A}[p]_{/\mathbf{Z}}$ is admissible. This factor $A_{/\mathbf{Q}}$ therefore satisfies the hypotheses of Theorem 3.1 and so has rank 0 over $\mathbf{Q}$.

References

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[Con95] Ian Connell, *Points of order* 11 *on elliptic curves*, Nieuw Arch. Wisk. (4) **13** (1995), no. 3, 257–288.

[Kub76] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.