p–descent and average ranks of elliptic curves

Frank Calegari

October 26, 1997

Abstract

Let $E/\mathbb{Q}$ be a semistable elliptic curve. For certain number fields K we bound the *rank* of $E(K)$ in terms of the *class number* of K. For a particular class of curves E, we prove that the average rank over all quadratic number fields is bounded.

1 Introduction

One of the most natural ways to understand the rank of an elliptic over K is to study its behavior locally at each completion K_v. Denote the K–rational points of E by E_K. Given a point $P \in E_K$ there exists a K_v–rational point $P_v \in E_{K_v}$ corresponding to the natural inclusion $K \hookrightarrow K_v$. The reverse of this principle, namely that if there exist non trivial K_v–rational points on E for all completions v then there exists a non trivial global point $P \in E_K$, does not hold in general (for examples, see [13]). In principle, however, one expects the obstruction (measured by the cohomological group $Ш(E/K)$) to be finite. In general, the method of *p–descent* considers the quotient group E_K/pE_K and its local equivalents, for which the obstruction to the "Hasse principle" is the p–group $Ш(E/K)[p]$. If one is lucky, and chooses p well, then this latter group vanishes, and one succeeds in calculating the order of E_K/pE_K. From the Mordell–Weil theorem this allows one to compute the rank of E_K, once the p–torsion has been determined. There are numerous difficulties with this method. Perhaps most significantly is that for $p \neq 2$ the above calculations become practically impossible. The ideas of Mazur [8] [9] [10] [11], however, make it feasible to carry out a first descent for certain p and E. Ironically, it is Mazur's main result in [10] that implies the set of such curves is empty for $p > 7$. The purpose of this note is to show that using bounds on the rank obtained in this way, one can prove (Theorems 4 and 5) unconditional density results about quadratic twists of certain elliptic curves.

2 Preliminaries

Let K be an algebraic number field, with ring of integers $\mathcal{O}_K$. Let E/K be an elliptic curve, and p an odd prime. We fix the following terminology. j_E is the j–invariant of E, and $\mathfrak{f}$ is the conductor. $\mathcal{E}$ denotes the Néron model of E, and $\mathcal{E}^0$ denotes the maximal connected component of $\mathcal{E}$ containing the identity. $\mathcal{E}[p]$ denotes the kernel of multiplication by p. $\mathcal{E}$ is a smooth group scheme over $\mathcal{S} = \text{Spec } \mathcal{O}_K$ with generic fiber E/K. We place the following restrictions on E and p:

1. E is *semistable.*
2. There exists a non–trivial point P on E_K of order p.
3. The number of components of the special fiber $\mathcal{E} \otimes_{\mathcal{S}} \overline{\mathbb{F}}_{\mathfrak{p}}$ for $\mathfrak{p}|\mathfrak{f}$ is divisible[1] by p.

Remark. The condition that E be semistable ensures that we have more control over the singular fibers. If $K = \mathbb{Q}$, it is a consequence of Mazur's theorem on rational torsion [9] [10] that $p \leq 7$.

Lemma 1 *Let $\mathfrak{p}$ be prime divisor of $\mathfrak{f}$. Let $v_{\mathfrak{p}}$ be a normalized valuation of $K_{\mathfrak{p}}$. Then the special fiber of $\mathcal{E}$ at $\mathfrak{p}$ has the following description:*

$$\mathcal{E} \otimes_{\mathcal{S}} \mathbb{F}_{\mathfrak{p}} \cong \mathcal{E}^0 \otimes_{\mathcal{S}} \mathbb{F}_{\mathfrak{p}} \times \mathbb{Z}/n\mathbb{Z}$$

where $n = -v_{\mathfrak{p}}(j_E)$, and $\mathcal{E}^0 \otimes_{\mathcal{S}} \mathbb{F}_{\mathfrak{p}}$ is of multiplicative type. Condition 3 *ensures that $p|n$.*

Proof. This follows immediately from Tate's algorithm [14] [15] and the fact that E is semistable.

3 Cohomology

All cohomology will be considered over the *fppf* site with base scheme $\mathcal{S} = \text{Spec } \mathcal{O}_K$ [4] [12]. It is necessary to work in this category rather than the étale site since the p–torsion $\mathcal{E}[p]$ will not in general be étale. Our main goal in this section will be to bound the size of $H^1(\mathcal{S}, \mathcal{E}[p])$. We begin by comparing $\mathcal{E}[p]$ with more familiar objects.

Lemma 2 *For any abelian group A, let $\text{rank}_p(A)$ denote the dimension of A/pA as a $\mathbb{Z}/p\mathbb{Z}$ vector space. Then*

$$\text{rank}_p(H^1(\mathcal{S}, \mathcal{E}[p])) \leq \text{rank}_p(H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z})) + \text{rank}_p(H^1(\mathcal{S}, \mu_p))$$

[1] With extra work, this condition may be ommited from our arguments—we include it mainly for ease of exposition. Condition 3 is also equivalent to j_E being a p^{th} power—this follows from Tate's algorithm [14].

Proof. From [8], Proposition 9.2, there is an exact sequence as follows:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{E}[p] \longrightarrow \mu_p \longrightarrow 0$$

The first map arises from the non–trivial torsion point of E_K. The second map is induced from the Weil paring. This sequence is naturally exact over the open subscheme $\mathcal{S}_{\mathfrak{f}} \subset \mathcal{S}$. It is harder to see that it is also exact at the singular fibers—however, this follows from Lemma 1. Taking global sections leads to the following exact sequence:

$$H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(\mathcal{S}, \mathcal{E}[p]) \longrightarrow H^1(\mathcal{S}, \mu_p)$$

The elementary properties of rank_p for finitely generated abelian groups now yields the lemma.

Remark. Without condition 3, μ_p must be replaced by a sheaf $\mu_{p!}$ whose restriction to $\mathcal{S}_{\mathfrak{f}}$ is $\mu_p|_{\mathcal{S}_{\mathfrak{f}}}$. There exists a $\mathfrak{g}|\mathfrak{f}$ such that if $j : \mathcal{S}_{\mathfrak{g}} \to \mathcal{S}$ is the natural inclusion, then $\mu_{p!} = j_! j^* \mu_p$ [8]. The cokernel Ψ of $\mu_{p!} \to \mu_p$ is a skyscraper sheaf with support on $\mathfrak{g}$, and $\mathrm{rank}_p(H^0(\mathcal{S}, \Psi))$ is bounded by the number of prime factors of $\mathfrak{g}$. From the long exact sequence of cohomology, $\mathrm{rank}_p(H^1(\mathcal{S}, \mu_{p!}))$ is then bounded by $\mathrm{rank}_p(H^1(\mathcal{S}, \mu_p))$ and a constant term arising from a factor of $\mathfrak{f}$. In this way Lemma 2 can be extended to the more general case—with an extra error term.

Having replaced $H^1(\mathcal{S}, \mathcal{E}[p])$ by more familiar objects, we now recall the calculation of their cohomology.

Theorem 1 (Hilbert's Theorem 90) *Let $\mathbb{G}_m$ denote the multiplicative group scheme over $\mathcal{S}$. Then there is an isomorphism*

$$H^1_{Zar}(\mathcal{S}, \mathcal{O}^*_{\mathcal{S}}) \longrightarrow H^1(\mathcal{S}, \mathbb{G}_m)$$

Proof. See [12], Proposition 4.9. This result is well known.

Since $\mathcal{S} = \mathrm{Spec}\ \mathcal{O}_K$, we may conclude [5] that

$$H^1(\mathcal{S}, \mathbb{G}_m) \cong \mathrm{Pic}(\mathcal{S}) \cong \mathrm{CL}(\mathcal{O}_K)$$

where $\mathrm{CL}(\mathcal{O}_K)$ is the class group of $\mathcal{O}_K$. Consider now the following sequence:

$$0 \longrightarrow \mu_p \longrightarrow \mathbb{G}_m \xrightarrow{p} \mathbb{G}_m \longrightarrow 0$$

This sequence *is* exact in the *fppf* topology. Taking cohomology yields the exact sequence

$$\Gamma(\mathcal{S}, \mathcal{O}_{\mathcal{S}})^* \xrightarrow{p} \Gamma(\mathcal{S}, \mathcal{O}_{\mathcal{S}})^* \longrightarrow H^1(\mathcal{S}, \mu_p) \longrightarrow H^1(\mathcal{S}, \mathbb{G}_m) \xrightarrow{p} H^1(\mathcal{S}, \mathbb{G}_m)$$

which from previous remarks and upon noting $\Gamma(\mathcal{S}, \mathcal{O}_{\mathcal{S}}) = \mathcal{O}_K^*$, yields the short exact sequence

$$0 \longrightarrow \mathcal{O}_K^*/\mathcal{O}_K^{*p} \longrightarrow H^1(\mathcal{S}, \mu_p) \longrightarrow \mathrm{CL}(\mathcal{O}_K)[p] \longrightarrow 0$$

Let β be the p–rank of $\mathrm{CL}(\mathcal{O}_K)$. Let K have r_1 real and $2r_2$ complex embeddings. From Dirichlet's unit theorem we find

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r_1+r_2-1} \oplus W_K$$

where W_K is the finite group of roots of unity inside K. The exact sequence above now tells us that

$$\mathrm{rank}_p(H^1(\mathcal{S}, \mu_p)) \leq \beta + r_1 + r_2 - 1 + \mathrm{rank}_p(W_K)$$

To evaluate the cohomology of $\mathbb{Z}/p\mathbb{Z}$, we note that it is already a *étale* sheaf. Hence by comparison theorems [12] (Theorem 3.9) for *fppf* and étale cohomology,

$$H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z}) \cong H^1_{\acute{e}t}(\mathcal{S}, \mathbb{Z}/p\mathbb{Z})$$

Etale covers of $\mathcal{S}$ are unramified extensions of $\mathcal{O}_K$. The above cohomology group corresponds to such extensions of degree p with given Galois action. Hence if H denotes the Hilbert class field of K, then

$$\mathrm{rank}_p(H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z})) = \mathrm{rank}_p(\mathrm{Hom}(\mathrm{Gal}(H/K), \mathbb{Z}/p\mathbb{Z})) = \mathrm{rank}_p(\mathrm{CL}(\mathcal{O}_K)[p]) = \beta$$

where we have identified $\mathrm{Gal}(H/K)$ with $\mathrm{CL}(\mathcal{O}_K)$ via class field theory.

4 p–Descent

We are now ready to compute the relevant descent on $\mathcal{E}$. We have an exact sequence of *fppf* sheaves over $\mathcal{S}$:

$$0 \longrightarrow \mathcal{E}[p] \longrightarrow \mathcal{E} \xrightarrow{\ p\ } \mathcal{E} \longrightarrow \Phi \longrightarrow 0$$

Multiplication by p is surjective away from the special fibers. Moreover, since E is semistable, the image of $\mathcal{E}$ contains the connected component $\mathcal{E}^0$ (since multiplication *is* surjective on multiplicative group schemes for the *fppf* site). Hence Φ is a skyscraper sheaf with support at the primes dividing $\mathfrak{f}$. Given our description of the special fibers, we may evaluate $H^0(\mathcal{S}, \Phi)$. Namely,

$$H^0(\mathcal{S}, \Phi) = \bigoplus_{\mathfrak{p}|\mathfrak{f}} (\mathbb{Z}/p\mathbb{Z})$$

and hence

$$\phi_{E/K} := \mathrm{rank}_p(H^0(\mathcal{S}, \Phi)) = \sum_{\mathfrak{p}|\mathfrak{f}} 1$$

Let $\mathcal{F}$ denote the image of $\mathcal{E}$ under p. In order to facilitate the use of cohomology, we write our exact sequence in the form

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}[p] \arrow[r] & \mathcal{E} \arrow[r, "\alpha"] \arrow[d, "\alpha"'] \arrow[dr, "p"] & \mathcal{F} \arrow[r] \arrow[d, "\beta"] & 0 & \\
& 0 \arrow[r] & \mathcal{F} \arrow[r, "\beta"'] & \mathcal{E} \arrow[r] & \Phi \arrow[r] & 0
\end{tikzcd}$$

Taking global sections over the base gives us the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}(\mathcal{O}_K)[p] \arrow[r] & H^0(\mathcal{S},\mathcal{E}) \arrow[r, "\alpha^*"] \arrow[d, "\alpha^*"'] \arrow[dr, "p"] & H^0(\mathcal{S},\mathcal{F}) \arrow[r] \arrow[d, "\beta^*"] & H^1(\mathcal{S},\mathcal{E}[p]) \\
& 0 \arrow[r] & H^0(\mathcal{S},\mathcal{F}) \arrow[r, "\beta^*"'] & H^0(\mathcal{S},\mathcal{E}) \arrow[r] & H^0(\mathcal{S},\Phi)
\end{tikzcd}$$

Taking into account that this diagram commutes we find

$$\mathrm{rank}_p(H^0(\mathcal{S},\mathcal{E})) \leq \mathrm{rank}_p(H^1(\mathcal{S},\mathcal{E}[p])) + \mathrm{rank}_p(H^0(\mathcal{S},\Phi))$$

Combining this with previous estimates, we may write:

$$\mathrm{rank}_p(H^0(\mathcal{S},\mathcal{E})) \leq 2\beta + r_1 + r_2 - 1 + \phi_{E/K} + \mathrm{rank}_p(W_K)$$

Since $H^0(\mathcal{S},\mathcal{E}) = \mathcal{E}(\mathcal{S}) = E_K$ (from the universal property of Néron models) we conclude (noting that E has non–trivial p–torsion) the following:

Theorem 2 *Let E/K be an elliptic curve such that*

1. *E is semistable.*
2. *$E[p]$ has a non–trivial point of order p over K.*
3. *j_E is a p^{th} power.*

Then

$$\mathrm{rank}(E_K) \leq 2\beta + r_1 + r_2 - 2 + \phi_{E/K} + \mathrm{rank}_p(W_K)$$

5 Applications and Examples

Let E be a semistable elliptic curve with a non–trivial point P of order p over $\mathbb{Q}$. Then E satisfies the conditions of Theorem 2 over any base, since multiplicative reduction is stable under base change. Moreover from Ogg's formula [14] we may compare the conductor $\mathfrak{f}$ of E/K with the conductor N of $E/\mathbb{Q}$, and hence evaluate $\phi_{E/K}$. Namely, let w_ℓ be the number of places in K above ℓ in $\mathbb{Q}$. Then

$$\phi_{E/K} = \sum_{\ell|N} w_\ell$$

We consider now *quadratic twists* of E, in particular over imaginary quadratic fields. Let $K = \mathbb{Q}(\sqrt{-D})$. In this case, $r_1 + r_2 - 1 = 0$, and $\mathrm{rank}_p(W_K) = 0$ unless $p = 3$ and $K = \mathbb{Q}(\sqrt{-3})$. Hence Theorem 2 yields (for $|\delta_K| > 3$) the estimate

$$\mathrm{rank}(E_K) \leq 2\beta - 1 + \phi_{E/K}$$

One such curve which satisfies the conditions of Theorem 2 is $E = X_0(19)$, with $j_E = -2^{18} \cdot 7^3/19^3$ and $p = 3$. We find that

$$\phi_{E,K} = \begin{cases} 2, & (\delta_K/19) = 1, \\ 1, & (\delta_K/19) = -1, \\ 1, & 19|\delta_K. \end{cases}$$

The densities of imaginary quadratic fields with these splitting conditions are 19/40, 19/40, and 1/20 respectively. The value of $\phi_{E/K}$ can be seen to correspond exactly to the sign of the functional equation for $L(E_K, s)$. Hence assuming the Birch–Swinnerton-Dyer conjecture[2], we have:

Corollary. If $3 \nmid h = |\mathrm{CL}(\mathcal{O}_K)|$, then $\mathrm{rank}(E_K)$ is 0 or 1 depending only on the sign of the functional equation.

Remark. When $\phi_{E/K} = 1$ our bounds suffice to prove this result unconditionally. An analogous result holds for $E = X_0(11)$ and $p = 5$, for which Mazur [11] proves a more refined version of the above.

The bounds on $\mathrm{rank}(E_K)$ suggest a natural way to look for twists of high rank—namely to consider quadratic fields K such that $\mathrm{CL}(\mathcal{O}_K)$ has a high p–rank.

Given our bounds on the rank for any quadratic field K, it is natural to ask whether we can bound the *expected* rank of E_K over all such fields (ordered in some natural way, such as by discriminant). Unfortunately, density results concerning the p–divisibility of class numbers are limited. If, however, we assume the Cohen–Lenstra heuristics [1] on the average p–rank of class numbers, we may construct such a bound. Let us restrict

[2] A 2–descent on E_K shows that we need only assume $Ш(E/K)$ has finite 2–primary component to infer that rank of E_K mod 2 is determined in this manner.

to the case $E = X_0(19)$. The Cohen–Lenstra heuristics in this case predict, that with $p = 3$, the probability that $\beta = k$ is equal to

$$\frac{p^{-k^2}(1/p)_\infty}{(1/p)_k^2}$$

Here we use $(q)_n$ to denote

$$\prod_{m=1}^{n}(1-q^m)$$

Hence, conjecturally at least, the average rank is bounded by the quantity

$$\frac{p}{2(1+p)} + 2(1/p)_\infty \sum_k \frac{kp^{-k^2}}{(1/p)_k^2} = 1.39448151730887504\ldots$$

Similar results can be obtained more generally under the assumption of the Generalized Riemann Hypothesis and the Birch–Swinnerton-Dyer conjecture [3]. For $X_0(19)$, however, we may replace the conjectures of Cohen–Lenstra with the theorems of Davenport–Heilbronn [2]. In particular we have

Theorem 3 (Davenport–Heilbronn) *Let δ_K denote a fundamental negative discriminant corresponding to the imaginary quadratic field K. Let β_K denote the corresponding 3–rank of $\mathrm{CL}(\mathcal{O}_K)$. Then*

$$\lim_{x\to\infty} \frac{\sum_{|\delta_K|<x} 3^{\beta_K}}{\sum_{|\delta_K|<x} 1} = 2$$

Our concern is the average value of $2\beta_K$. Using the inequality $1 + 2\beta \leq 3^\beta$ for $\beta \in \mathbb{N}$ we infer that:

Theorem 4 *Let $E = X_0(19)$. Then the average rank of E_K over all imaginary quadratic fields (ordered by discriminant) is less than $59/40$.*

Of course this analysis applies only to the single curve $X_0(19)$! However, the same analysis suffices to prove the following.

Theorem 5 *Let E be an elliptic curve such that*

- *E is semistable.*
- *E has a rational non–trivial torsion point of order three.*

Then the average rank of E_K over all imaginary quadratic fields ordered by discriminant is bounded by an explicitly computable constant depending only on the number of prime divisors of N.

Remark. The same result applies to real quadratic fields, since there is a corresponding Davenport–Heilbronn theorem in that case.

These ideas also yield information on curves of rank 0.

Theorem 6 *Let E be an elliptic curve satisfying the conditions of the previous theorem. Suppose moreover that j_E is a perfect cube, and N is prime. Then* $\mathrm{rank}(E_K) = 0$ *for a positive proportion of imaginary quadratic fields K.*

Proof. From Theorem 2, we conclude that

$$\mathrm{rank}(E_K) \leq 2\beta$$

for any imaginary quadratic field K in which N remains inert. By Ĉebotarev, the set of such fields has positive density over all quadratic extensions. Hence it suffices to prove that a positive proportion of such fields have class number coprime to 3. This follows from the more general version of Theorem 3, in which the summation over all discriminants is replaced by a summation over $|\delta_K| < x$ satisfying a certain Kronecker relation.

Remark. The previous Theorem applies in particular to $X_0(19)$. Naturally the result also applies to any curve isogenous to E over $\mathbb{Q}$. The next smallest example arises from the component of $J_0(37)$ corresponding to eigenvalue -1 under the Fricke involution.

So far we have considered only the case $[K : \mathbb{Q}] = 2$. Our ideas however can be applied more generally—including both more curves and fields of higher degree.

6 Average Ranks over arbitrary fields

We will consider elliptic curves over algebraic number fields K of degree n. We make the following assumption:

- E is semistable.

We have the following result.

Theorem 7 *Suppose that Cohen–Lenstra–Martinet heuristics apply to general classes of number fields of degree n. Then the average rank of E over all fields K of degree n (ordered by discriminant) is bounded.*

Sketch of Proof. We shall be more specific on what we mean by general "Cohen–Lenstra–Martinet" heuristics below. It suffices to prove the theorem for n sufficiently large. After a base change if necessary, we may assume that E has a rational p–division point. Hence by [8] Proposition 9.2, we obtain an exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{E}[p] \longrightarrow \mu_{p!} \longrightarrow 0$$

with $\mu_{p!}$ defined as in section three. In this context we may bound (as before) the cohomology of $\mathcal{E}[p]$ in terms of $H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z})$ and $H^1(\mathcal{S}, \mu_p)$, with a certain controlled error term. Write the base scheme as Spec $\mathcal{O}_L$, for some number field L determined by the above process. Let K be a field of degree n, and let $L \cup K$ denote the compositum. Let $\mathcal{S} =$ Spec $\mathcal{O}_{K\cup L}$. Then we may recompute the exact sequences of section four to obtain an estimate of the form:

$$\mathrm{rank}_p(E_K) \leq c(E,n) + \dim_p(H^1(\mathcal{S}, \mathcal{E}[p])) + \dim_p(H^0(\mathcal{S}, \Phi))$$

This last term is determined by the splitting of N in $L \cup K$—hence it is bounded for all K by some constant $e(E,n)$, since the degree of $L \cup K$ is itself less than $n \cdot [L:\mathbb{Q}]$. Absorb this term into $c(E,n)$. Our cohomological calculations of $H^1(\mathcal{S}, \mathbb{Z}/p\mathbb{Z})$ and $H^1(\mathcal{S}, \mu_p)$ remain valid. Since $r_1 + r_2 - 1 \leq n - 1$ we infer the estimate

$$\mathrm{rank}(E_K) \leq \mathrm{rank}(E_{K\cup L}) \leq c(E,n) + n - 1 + 2\beta + \mathrm{rank}_p(W_{L\cup K})$$

where $\beta = \mathrm{rank}_p(\mathrm{CL}(\mathcal{O}_{K\cup L}))$. Note that $\mathrm{rank}_p(W_{L\cup K})$ is bounded independently of K. To finish the proof, it suffices to show that

$$\lim_{x\to\infty} \frac{\sum_{|\delta_K|<x}^{[K:\mathbb{Q}]=n} \beta_{K\cup L}}{\sum_{|\delta_K|<x}^{[K:\mathbb{Q}]=n} 1} < \infty$$

General arguments of the Cohen–Lenstra–Martinet type would imply that this limit exists even when β is replaced by p^β. However, the explicit claim above has not been proven for any case besides $L = \mathbb{Q}$, $p = 3$, and $n = 2$.
Corollary. Let E, E' be two elliptic curves with $j_E = j_{E'}$ such that E is semistable. Then the theorem above applies to E'.
Proof. After a base change if necessary, $\mathcal{E} \cong \mathcal{E}'$. The result follows.

Note that this result does not cover all elliptic curves—for instance a curve with integral j–invariant cannot be semistable, so the result will not apply in this case. No doubt, however, a more refined analysis will indicate the same result as above for *all* elliptic curves.

7 Remarks and Further Questions

I believe that Theorems 4, 5 and 6 are the first unconditional result of their type. It should be kept in mind, however, that the methods we use to bound the rank of E_K are very primitive. In particular, we consider little of the particular structure of E, and we ignore more subtle questions about the Tate–Shafarevich group, proper consideration of which will undoubtably give more interesting results.

This work was motivated by an attempt to understand the conjectures in [7], where curves of the form

$$x^3 + y^3 = m$$

tended to produce more than the *a priori* expected number of curves of rank 2.

It is still unclear at yet what the *conjectural* average rank of E over quadratic twists should be.

8 Acknowledgments

I would like to thank Matthew Emerton, Mark Kisin, and Professors Gerd Faltings and Doug Ulmer for some technical help concerning cohomology. Thanks also to Annette Werner who corrected a few ommisions in a earlier version of this manuscript.

This work was done during a pleasant one month stay at the Max–Planck–Institute für Mathematik in Bonn.

References

[1] H. Cohen, H. W. Lenstra. *Heuristics on Class groups of number fields*, Springer–Verlag, LNM 1068. (1983) pp. 33–62.

[2] H. Davenport, H. Heilbronn. *On the density of discriminants of cubic fields*, Bull. London Math. Soc. 1 (1969) pp. 345–348.

[3] D. Goldfeld. *Conjectures on Elliptic Curves over Quadratic Fields*, Springer–Verlag, LNM 751. (1979).

[4] A. Grothendieck *Revêtements étales et groupes fondamentaux. Séminaires de Géometrie Algébrique*, Springer–Verlag, LNM 224. (1960-61).

[5] R. Hartshorne. *Algebraic Geometry*, Springer–Verlag, GTM 52. (1977).

[6] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*, Springer–Verlag, GTM 97. (1984).

[7] G. Kramarz, D. Zagier. *Numerical Investigations related to the L–series of certain elliptic curves*, J. Indian Math. Soc. (N.S) 52, (1988) pp. 51-69.

[8] B. Mazur. *Rational points of Abelian varieties with values in towers of number fields*, Inventiones Mathematicæ, Springer–Verlag, 18, (1972) pp. 183–266.

[9] B. Mazur. *Rational points on elliptic curves*, Springer–Verlag. LNM 601. (1976) pp. 108–148.

[10] B. Mazur. *Modular curves and the Eisenstien ideal*, I.H.E.S. 47. (1977) pp. 33–186.

[11] B. Mazur. *On the arithmetic of special values of L–functions*, Inventiones Mathematicæ, Springer–Verlag, 55, (1977) pp. 207–240.

[12] J.S. Milne. *Introduction to étale cohomology*, Princeton University Press. (1980).

[13] J. Silverman. *The Arithmetic of Elliptic Curves*, Springer–Verlag, GTM 102. (1986).

[14] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer–Verlag, GTM 151. (1994).

[15] J. Tate. *Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil*, in "Modular Functions of one Variable IV", Springer–Verlag, LNM 476. (1972).