The exponents of the groups of points on the reductions of an elliptic curve

René Schoof

Mathematisch Instituut
Rijksuniversitiet Utrecht
3508 TA Utrecht
The Netherlands

Abstract. Let E denote an elliptic curve over $\mathbf{Q}$ without complex multiplication. It is shown that the exponents of the groups $E(\mathbf{F}_p)$ grow at least as fast as $\frac{\sqrt{p}\log p}{(\log\log p)^2}$.

1. Introduction.

The exponent $\exp(A)$ of a finite abelian group A is the smallest positive integer m for which $ma = 0$ for all $a \in A$. In this note we study the exponents of the groups $E(\mathbf{F}_p)$ of points modulo a prime of good reduction p of an elliptic curve E which is defined over $\mathbf{Q}$.

By the Riemann hypothesis for elliptic curves over finite fields [7, Ch.5.Thm.1.1], proved by H. Hasse in 1933, we have that

$$|\#E(\mathbf{F}_p) - (p+1)| < 2\sqrt{p}.$$

Since the group $E(\mathbf{F}_p)$ can be generated by two points [7, Ch.3.Cor.6.4] we see that

$$\sqrt{p} - 1 < \exp(E(\mathbf{F}_p)) < (\sqrt{p} + 1)^2.$$

In this note we show that for elliptic curves without complex multiplication the lower bound can be somewhat improved:

Theorem 1.1. *Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication. There exists a constant $C_E > 0$ such that*

$$\frac{\exp(E(\mathbf{F}_p))}{\sqrt{p}} > C_E \frac{\log p}{(\log\log p)^2}$$

for every prime p of good reduction.

Note that "complex multiplication" means complex multiplication over $\mathbf{C}$. Theorem 1.1 is proved in section 2. It is a consequence of the fact that the absolute values of the discriminants Δ_p of the endomorphism rings of the curve $E \pmod{p}$ grow as p goes to infinity. We show that

$$|\Delta_p| \geq C'_E \frac{(\log p)^2}{(\log \log p)^4}$$

for some constant $C'_E > 0$.

In section 3 we investigate how small the exponents $\exp(E(\mathbf{F}_p))$ and the discriminants Δ_p can be. Assuming certain generalized Riemann Hypotheses we can show that there exists a constant c_E so that for infinitely many primes p the quantity $\exp(E(\mathbf{F}_p))/\sqrt{p}$ is less than $c_E p^{3/8} \log p$. Similarly we can show that there exists a constant c'_E such that $|\Delta_p| \leq c'_E p^{3/4} \log p$ for infinitely many primes p.

I would like to thank Hendrik Lenstra for the elegant proof of Lemma 2.1 and the referee for many helpful suggestions.

2. Large exponents.

In this section we prove Theorem 1. We need two lemmas.

Lemma 2.1. *Let R be a quadratic order of discriminant Δ and let $\chi(x)$ denote the quadratic residue symbol $(\frac{\Delta}{x})$. Let furthermore ℓ be a prime and let O denote $R \otimes \mathbf{Z}_\ell$. We have*

$$\sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}} = \frac{\ell+1}{\ell - \chi(\ell)},$$

where the sum runs over all invertible ideals $\mathfrak{a}$ in O which are not contained in ℓO. The norm $N\mathfrak{a}$ is just $\#R/\mathfrak{a}$.

Proof. When $\chi(\ell) = 1$ he ring O is isomorphic to a $\mathbf{Z}_\ell \times \mathbf{Z}_\ell$, when $\chi(\ell) = -1$ it is a local ring with maximal ideal generated by ℓ and when $\chi(\ell) = 0$ it is a local ring with maximal ideal $\mathfrak{l}$ of index ℓ.

Let μ denote a Haar measure on O. We have

$$\mu(O^*) = \mu(\mathbf{Z}_\ell^*)^2 = (1 - \frac{1}{\ell})^2 \mu(O) \qquad \text{if } \chi(\ell) = 1.$$

$$= \mu(O) - \mu(\ell O) = (1 - \frac{1}{\ell^2})\mu(O) \qquad \text{if } \chi(\ell) = -1,$$

$$= \mu(O) - \mu(\mathfrak{l}) = (1 - \frac{1}{\ell})\mu(O) \qquad \text{if } \chi(\ell) = 0,$$

In other words

$$\mu(O^*) = (1 - \frac{1}{\ell})(1 - \frac{\chi(\ell)}{\ell})\mu(O). \qquad (1)$$

The ring O is a disjoint union of ℓO, the zero divisors not in ℓO and sets of the form αO^* where α is not a zero divisor and α is not contained in ℓO. Since the zero divisors have

measure zero we find that

$$\mu(O) = \mu(\ell O) + \sum_\alpha \mu(\alpha O^*).$$

Therefore

$$(1 - \frac{1}{\ell^2})\mu(O) = \mu(O^*) \sum_\alpha \frac{1}{N\alpha}$$

and hence by (1) that

$$\sum_\alpha \frac{1}{N\alpha} = \frac{\ell + 1}{\ell - \chi(\ell)}$$

where the summation runs over $\alpha \in O - \ell^2 O$ which are not zero divisors; they are counted modulo units of O. Since O is a semi-local ring the invertible O-ideals are precisely the ideals of the form αO where α is not a zero divisor. The result now follows at once.

It was pointed out by the referee that the following lemma on binary quadratic forms can also be proved in an elementary way i.e. without invoking Lemma 2.1.

Lemma 2.2. *There exists an absolute constant C such that for every $\Delta \in \mathbf{Z}_{<0}$ congruent to 0 or 1 (mod 4) we have that*

$$\sum \frac{1}{a} \leq C \log^2 |\Delta|$$

where the sum runs over all reduced positive definite primitive binary quadratic forms $aX^2 + bXY + cY^2$ of discriminant Δ.

Proof. It is easy to see that for a reduced positive definite quadratic form $aX^2 + bXY + cY^2$ one has that $a \leq \sqrt{|\Delta|/3}$. Using the dictionary between quadratic forms of discriminant Δ and ideals in the order of discriminant Δ one sees that

$$\sum \frac{1}{a} = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}}$$

where the second summation runs over all invertible ideals $\mathfrak{a}$ in the order of discriminant Δ which are *primitive* and have their norms not exceeding $\sqrt{|\Delta|/3}$. Here an ideal in an order R is called primitive if it is not contained in mR for any integer $m > 1$.

Decomposing the ideals into products of prime ideals one finds that this sum does not exceed

$$\prod_\ell \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}}.$$

Here the product runs over the primes ℓ less than $\sqrt{|\Delta|/3}$ and the sums run over all primitive ideals $\mathfrak{a}$ having norm a power of ℓ. The sums can be computed in the semi-local rings $R \otimes \mathbf{Z}_\ell$. Therefore we obtain as an application of lemma 2.1 that

$$\sum \frac{1}{a} \leq \prod_\ell \frac{\ell + 1}{\ell - \chi(\ell)} \leq \prod_\ell (1 - \frac{1}{\ell})^{-2}.$$

3

By Mertens's Theorem [4,Thm 429] the product $\prod(1-\frac{1}{\ell})^{-1}$ is $O(\log\sqrt{|\Delta|/3})$ and therefore we find that $\sum\frac{1}{a} \leq C\log^2|\Delta|$ for some universal constant C. This proves the lemma.

For $z \in \mathbf{C}$ with $\mathrm{Re}z > 0$ let $j(z)$ denote the modular function

$$j(z) = \frac{(1 + 240\sum_{n=1}^{\infty}\frac{n^3 q^n}{1-q^n})^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}$$

where q denotes $e^{2\pi iz}$. The Fourier expansion of the j-functions begins as $q^{-1} + 744 + 196884q + \ldots$. For z in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane the quantity $|qj(z)|$ is bounded. In fact, it is easy to see that there exists a constant $C \in \mathbf{R}$ such that $|qj(z)| < C$ for all $z \in \mathbf{C}$ satisfying $\mathrm{im}z \geq \frac{1}{2}\sqrt{3}$.

Proposition 2.4. *Let $\Delta \in \mathbf{Z}< 0$ be congruent to 0 or 1 (mod 4) and let $n, m \in \mathbf{Z}$. Then*

$$\prod_{aX^2+bXY+cY^2} |m - n \cdot j(\frac{-b+i\sqrt{|\Delta|}}{2a})| \leq e^{C\sqrt{|\Delta|}\log^2|\Delta|},$$

where C is a constant depending only on n and m. The product runs over the $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of positive definite primitive binary quadratic forms of discriminant Δ.

Proof. A quadratic form $aX^2 + bXY + cY^2$ of discriminant Δ is reduced if and only if the number $\frac{-b+i\sqrt{|\Delta|}}{2a}$ is in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane. Therefore we have, for some absolute constants C and C_1, that

$$|m - n \cdot j(\frac{-b+i\sqrt{|\Delta|}}{2a})| \leq |m| + |n|C|q|,$$
$$\leq C_1\max(|n|,|m|)e^{\frac{\pi\sqrt{|\Delta|}}{a}}.$$

Every equivalence class contains exactly one reduced form and we conclude that

$$\prod |m - n \cdot j(\frac{-b+i\sqrt{|\Delta|}}{2a})| \leq (C_1\max(|n|,|m|))^{h(\Delta)}e^{\pi\sqrt{|\Delta|}\sum\frac{1}{a}}.$$

For a reduced form $aX^2 + bXY + cY^2$ one has that $a \leq \sqrt{|\Delta/3|}$. Therefore it follows at once from Lemma 2.2 that there is a constant C_2 such that the class number $h(\Delta)$ is bounded by $C_2\sqrt{|\Delta|}\log|\Delta|$ for all Δ. By Lemma 2.2 there exists an absolute constant C_3 such that $\sum\frac{1}{a} \leq C_3\log^2|\Delta|$. This implies that

$$\prod |m - n \cdot j(\frac{-b+i\sqrt{|\Delta|}}{2a})| \leq (C_1\max(|n|,|m|))^{C_2\sqrt{|\Delta|}\log^2|\Delta|}e^{C_3\pi\sqrt{|\Delta|}\log^2|\Delta|}$$
$$\leq e^{C_4\sqrt{|\Delta|}\log^2|\Delta|}.$$

4

for some absolute constant C_4. This proves the proposition.

Corollary 2.4. *Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication. For every prime p of good reduction let Δ_p denote the discriminant of the endomorphism ring of the reduced curve $E_{/\mathbf{F}_p}$. There exists a constant $C'_E > 0$ such that*

$$|\Delta_p| > C'_E \frac{(\log p)^2}{(\log\log p)^4} \qquad \text{for all } p.$$

Proof. We may assume that $p \geq 5$. If p is a prime of supersingular reduction we have that $\Delta_p = -p$ or $-4p$ and we are done. If p is a prime of ordinary reduction we observe that the j-invariant $j(E)$ of the curve E is congruent to the j-invariant $j_p \in \overline{\mathbf{Q}}$ of an elliptic curve with complex multiplication by the quadratic order of discriminant Δ_p. We conclude, since $j(E) - j_p$ is not zero, that $p \leq \prod |n - mj'|$ where n and m are integers such that $j(E) = n/m$ and where the product runs over the conjugates j' of j_p. These conjugates are precisely the $j(\frac{-b+i\sqrt{|\Delta|}}{2a})$ with $aX^2 + bXY + cY^2$ a primitive binary quadratic form of discriminant Δ_p. It follows from Proposition 2.3 that

$$p \leq e^{C\sqrt{|\Delta_p|}\log^2|\Delta_p|}$$

which easily implies the required result.

Proof of Theorem 1.1. We may assume that $p \geq 5$ and that p is a prime of good reduction. Let Δ_p denote the discriminant of the ring of endomorphisms O of E over $\mathbf{F}_p$. We write

$$E(\mathbf{F}_p) \cong \mathbf{Z}/nd\mathbf{Z} \oplus \mathbf{Z}/d\mathbf{Z}$$

so that $\exp(E(\mathbf{F}_p)) = nd$. We have

$$\exp(E(\mathbf{F}_p))^2 = n^2 d^2 = n\#E(\mathbf{F}_p) \geq n(\sqrt{p}-1)^2$$

by Hasse's inequality. Since the d-torsion points of E are defined over $\mathbf{F}_p$ we must have that

$$\phi_p = 1 + d\psi \qquad \text{for some } \psi \in O.$$

Since $\phi_p \notin \mathbf{Z}$ the endomorphism ψ is not in $\mathbf{Z}$ either and we find that

$$nd^2 = \#E(\mathbf{F}_p) = (\phi - 1)(\bar{\phi} - 1) = d^2\psi\bar{\psi} \geq d^2 \frac{|\Delta_p|}{4}.$$

Therefore $n \geq \frac{|\Delta_p|}{4}$ and we get

$$\exp(E(\mathbf{F}_p)) \geq \frac{1}{2}\sqrt{|\Delta_p|}(\sqrt{p}-1).$$

The result now follows at once from Corollary 2.4.

Remark 2.6. Theorem 1.1 is very probably false when the elliptic curve E has complex multiplication: consider the elliptic curve given by $Y^2 = X^3 - X$. It has complex multiplication by the ring $\mathbf{Z}[i]$. This curve has its 2-torsion points rational over $\mathbf{Q}$ while the field of definition of the 4-torsion points is $\mathbf{Q}(\zeta_8)$, the field of 8th roots of unity. We conclude that for primes p that are congruent to 1 (mod 8), the Frobenius endomorphism ϕ_p is congruent to 1 (mod 4) in $\mathbf{Z}[i]$.

Suppose p is an odd prime of the form $n^2 + 1$. In this case n is even and p splits in $\mathbf{Z}[i]$ as $(1 - ni)(1 + ni)$. Therefore the Frobenius endomorphism ϕ_p of a prime like this must be one of $\pm 1 \pm ni$ or $\pm i \pm n$. One concludes that for primes p of the form $n^2 + 1$ with $n \equiv 0$ (mod 4) one has that $\phi_p = 1 \pm ni$ and

$$E(\mathbf{F}_p) \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$$

showing that $\exp(E(\mathbf{F}_p)) = n \approx \sqrt{p}$. Since it is very likely that there are infinitely many primes of the form $n^2 + 1$ with $n \equiv 0$ (mod 4), it is also likely that Theorem 1.1 is false for elliptic curves with complex multiplication. It is easy to show that certain standard conjectures on the distribution of prime numbers in quadratic progressions imply that for every elliptic curve E over $\mathbf{Q}$ with complex multiplication the exponent of $E(\mathbf{F}_p)$ is $\sqrt{p} + o(1)$ for infinitely many primes p. It would be interesting to try and show without any unproved hypotheses that for elliptic curves over $\mathbf{Q}$ with complex multiplication there exist infinitely many primes p for which $\exp(E(\mathbf{F}_p))/\sqrt{p}$ is bounded.

3. Small exponents.

In this section we show that for an elliptic curve E over $\mathbf{Q}$ there exist infinitely many primes p for which $\exp(E(\mathbf{F}_p))$ is relatively small. We derive the results from an effective Čebotarev Density Theorem. A strong and realistic version of this theorem can at present only be proved assuming the truth of certain Generalized Riemann Hypotheses (GRH). Propositions 3.3 and 3.4 are only valid under these hypotheses.

Let K be a finite Galois extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(K/\mathbf{Q})$. The discriminant of K is denoted by Δ_K and we let $\delta_K = |\Delta_K|^{1/n}$ where $n = [K : \mathbf{Q}]$ denote the root discriminant of K. For a prime p let e_p denote the ramification index of p in K over $\mathbf{Q}$ and let r_p denote $v_{\mathfrak{p}}(\mathfrak{D}_{K/\mathbf{Q}})$; here $\mathfrak{D}_{K/\mathbf{Q}}$ denotes the different of K over $\mathbf{Q}$ and $v_{\mathfrak{p}}$ denotes the normalized valuation associated to a prime $\mathfrak{p}$ over p in K. It is elementary to check that

$$\delta_K = \prod_p p^{r_p/e_p},$$

where the product runs over all primes p.

Prposition 3.1. *Let E be an elliptic curve over $\mathbf{Q}$ and let ℓ be a prime. By K we denote the field generated by the group of ℓ-torsion points $E[\ell]$. We have*

$$\delta_K < |\Delta_E|\ell^2;$$

here Δ_E denotes the discriminant of the curve E.

Proof. The field K is a Galois extension of $\mathbf{Q}$. We put $G = \mathrm{Gal}(K/\mathbf{Q})$. Using the notation introduced above we have that $r_p/e_p = 0$ for every unramified prime p. We now estimate the ratios r_p/e_p for all primes p that ramify in K over $\mathbf{Q}$.

6

case 1. $p \neq \ell$. Since the prime p is ramified in K, it must be a prime of bad reduction. We use Ogg's formula [6]:

$$\text{ord}_p \Delta_E = \#C + \epsilon + \delta - 1,$$

where C denotes the set of components of the Néron minimal model of E over $\mathbf{Z}$ and $\epsilon = 1$ or 2 according as the reduced curve $E \pmod p$ has a double point or a cusp singularity. In either case we have

$$\text{ord}_p \Delta_E \geq \delta + 1,$$

where δ is Serre's measure of wild ramification [6]:

$$\delta = \frac{1}{e_p} \sum_{j=1}^{\infty} \#G_j \ \text{codim}(\text{E}[\ell]^{\text{G}_j}).$$

Here $G_j = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathfrak{p}^j} \text{ for all integral } x\}$ denotes the j-th higher ramification group. Let i denote the largest integer for which $G_i \neq \{1\}$. We clearly have

$$\delta \geq \frac{1}{e_p} \sum_{j=1}^{i} \#G_j.$$

Therefore

$$r_p = v_{\mathfrak{p}}(\mathfrak{D}_{K/\mathbf{Q}}) = \sum_{j=0}^{\infty} (\#G_j - 1) \leq e_p - 1 + e_p \delta < e_p \text{ord}_p \Delta_E$$

and hence

$$\frac{r_p}{e_p} < \text{ord}_p \Delta_E.$$

case 2. $p = \ell$. If ℓ is tamely ramified in K we clearly have that

$$\frac{r_\ell}{e_\ell} = 1 - \frac{1}{e_\ell} < 2.$$

If ℓ is wildly ramified we let $\mathfrak{l}$ denote a prime over ℓ in K and we consider the local field extension $K_{\mathfrak{l}}$ over $\mathbf{Q}_\ell$ with Galois group G_ℓ. The group G_ℓ considered as a subgroup of $GL_2(\mathbf{F}_\ell)$ contains the subgroup $N = \{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbf{F}_\ell \}$ as a normal subgroup. Therefore G_ℓ is contained in the normalizer of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which is the group of upper triangular matrices. By the non-degeneracy of the Weil-pairing the determinant maps G/N onto $(\mathbf{Z}/\ell\mathbf{Z})^*$ and we find that $K_{\mathfrak{l}}$ is a cyclic extension of degree ℓ of the field $F(\zeta_\ell)$ where F is an unramified extension of $\mathbf{Q}_\ell$. By local class field theory the conductor of $K_{\mathfrak{l}}$ over $F(\zeta_\ell)$ is at most $(\zeta_\ell - 1)^{\ell+1}$. One easily checks that $r_\ell \leq 2\ell^2 - 2\ell - 1$ and, since $e_\ell \leq \ell(\ell-1)$, that

$$\frac{r_\ell}{e_\ell} < 2.$$

Combining everything we obtain

$$\delta_K < |\Delta_E|\ell^2$$

as required.

Remark 3.2. When E has good reduction at ℓ one has in fact that

$$\delta_K < |\Delta_E|\ell^{1+\frac{1}{\ell-1}}$$

(see [3].) The result in Prop.3.1 is sufficiently strong for our purposes.

Assuming the Generalized Riemann Hypotheses (*GRH*) we can now show the following:

Proposition 3.3. *(Assuming GRH) Let E be an elliptic curve over $\mathbf{Q}$. There exists a constant c_E such that*

$$\frac{\exp(E(\mathbf{F}_p))}{\sqrt{p}} < c_E p^{3/8} \log p$$

for infinitely many primes p.

Proof. Let ℓ be a prime and let K denote the field generated by the ℓ-torsion points of E. Since the cardinality of $G = \mathrm{Gal}(K/\mathbf{Q})$ is at most $\#GL_2(\mathbf{F}_\ell) < \ell^4$, Proposition 3.1 implies that the discriminant Δ_K of K satisfies

$$|\Delta_K| \le |\Delta_E \ell^2|^{\ell^4}.$$

Therefore the effective Čebotarev Density Theorem [5] implies that there exists a prime $p < c\ell^8 \log^2 |\Delta_E \ell^2|$ that splits completely in K. Here c denotes some absolute constant. The ℓ-torsion points are rational over $\mathbf{F}_p$. Therefore

$$\exp(E(\mathbf{F}_p)) \le \frac{(\sqrt{p}+1)^2}{\ell}$$

which is easily seen to imply that

$$\frac{\exp(E(\mathbf{F}_p))}{\sqrt{p}} \le c_E p^{3/8} \log p$$

for some constant c_E that only depends on E. Letting $l \longrightarrow \infty$, one finds infinitely many primes this way, the result follows.

Proposition 3.4. *(Assuming GRH) Let E be an elliptic curve over $\mathbf{Q}$. There exists a constant c_E' such that*

$$|\Delta_p| < c_E' p^{2/3} \log p$$

for infinitely many primes p.

Proof. Let ℓ be a prime and let K be the field that appears in the proof of the previous proposition. Let K' denote the subfield of K that is invariant under the centre of $GL_2(\mathbf{F}_\ell)$. Then we have $[K' : \mathbf{Q}] \leq \#\mathrm{PGL}_2(\mathbf{F}_\ell) < \ell^3$ and therefore

$$|\Delta_{K'}| \leq |\Delta_E \ell^2|^{\ell^3}.$$

By Čebotarev there exists therefore a prime $p < c\ell^6 \log^2 |\Delta_E \ell^2|$ that splits completely in K'. The Frobenius endomorphism ϕ_p of p is congruent to an integer $\pmod{\ell}$ in $\mathrm{End}(E_{/\mathbf{F}_p})$. Therefore we have $\frac{|\Delta_p|}{4} \ell^2 \leq p$ and it follows easily that

$$|\Delta_p| \leq c'_E p^{2/3} \log p$$

for some constant c'_E which only depends on E. This proves Prop.3.4.

Conjecture 3.5. It seems reasonable to conjecture that for infinitely many primes ℓ as in Propositions 3.3 and 3.4 one can find primes p completely splitting in K or K' which do not exceed $\log |\Delta_K|$ or $\log |\Delta_{K'}|$ respectively. This would imply that

$$\frac{\exp(E(\mathbf{F}_p))}{\sqrt{p}} \leq c_E p^{1/4} \log p$$

and

$$|\Delta_p| \leq c'_E p^{1/3} \log p$$

for infinitely many primes p.

This conjecture seems to be related to an elliptic analogue of the problem of estimating the largest prime divisor of $p - 1$, see [2]. I have no idea how the exponents and the $|\Delta_p|$ are distributed as p varies.

Bibliography

[1] Davenport, H.:*Multiplicative Number Theory* (second edition), Graduate Texts in Math. **74**, Springer-Verlag, New York 1980.
[2] Deshouillers, J.-M.: Théorème de Fermat: La contribution de Fouvry. *Sém. Bourbaki, exp. 648 (juin 1985)*. Astérisque **133/134**, (1986), 309–318.
[3] Fontaine, J.-M.: Il n'y a pas de variété abélienne sur **Z**, *Invent. Math.* **81**, (1985), 515–538.
[4] Hardy, G. and Wright, E.: *An Introduction to the Theory of Numbers*, Oxford Univ. Press, Oxford 1960.
[5] Lagarias, J.C., Montgomery, H.L. and Odlyzko, A.M.: A Bound for the Least Prime Ideal in the Chebotarev Density Theorem, *Invent. Math.* **54**, (1979), 271–296.
[6] Ogg, A.: Elliptic curves and wild ramification, *Amer J. of Math.* **89**, (1967), 1–21.
[7] Silverman, J.: *The Arithmetic of Elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag, New York 1986.