On Elliptic Curves and Arithmetical Graphs

by

Jeremiah Hower

(Under the direction of Dino Lorenzini)

Abstract

Brumer and Kramer give sufficient criteria to conclude for a given prime p the non-existence of an elliptic curve $E/\mathbb{Q}$ of conductor p. Some of these criteria arise out of how primes factor in the 2-division and 3-division fields of the elliptic curve. In this paper we take a similar approach except instead of $\mathbb{Q}$ our base field is any one of the (exactly 9) class number 1 quadratic imaginary number fields. For a certain 6 of these number fields we are able, in each case, to exhibit a long list of prime numbers less than 500 that are residual characteristics of prime ideals for which we have a non-existence result. We then relate these non-existence results to a conjecture of Cremona.

A new invariant, called the g-integer, of an arithmetical graph is introduced by Lorenzini. Here we determine the effect on this invariant under basic operations on the arithmetical graph. We then focus on the case of arithmetical trees whose g-integer is 0 or 1. Moreover, we compute this invariant for certain modular curves.

Index words: Elliptic Curves, Arithmetical Graphs

On Elliptic Curves and Arithmetical Graphs

by

Jeremiah Hower

B.S., Virginia Polytechnic Institute and State University, 2003
M.A., University of Georgia, 2008

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2009

On Elliptic Curves and Arithmetical Graphs

by

Jeremiah Hower

Approved:

Major Professor: Dino Lorenzini

Committee: Daniel Nakano
Robert Rumely
Robert Varley

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2009

Acknowledgments

I would like to thank Dino Lorenzini for his suggesting to explore the methods in this paper. His comments, recommendations, and advice regarding this work are valuable and immensely appreciated. In addition, I thank my family, especially my wife, for the love and support given to me.

Table of Contents

Chapter 1

Introduction

This dissertation consists of work on two distinct projects. The first focuses on a problem related to elliptic curves while the second looks at an invariant of arithmetical graphs. We start by summarizing the former.

Different techniques have been used to prove when an elliptic curve, over a number field, of prime conductor cannot exist. In [Set] it is shown that, over $\mathbb{Q}$, there is an elliptic curve with a rational point of order 2 and with prime conductor $p \notin \{2,3,17\}$ exactly when $p-64$ is a square. The successful method involved, which is to determine whether some Diophantine equations have a solution, was given an analogous attempt, over the class number 1 quadratic imaginary number fields, $\mathbb{Q}(\sqrt{-d})$ for $d \in \{1,2,3,7,11,19,43,67,163\}$, by Shumbusho in [Shu]. For five of these fields this attempt produced, along with class field theory, ideals that could never be the conductors of prime conductor elliptic curves.

In [B-K] a different direction for the study of elliptic curves, over $\mathbb{Q}$, of prime conductor is taken. There, an analysis, broken into cases according to the reduction type at 3, is made on class number related restrictions for $\mathbb{Q}(\Delta^{\frac{1}{3}})$ (the field gotten by adjoining a cube root of the discriminant of the curve) and ramification related restrictions for $\mathbb{Q}(\Delta^{\frac{1}{3}})/\mathbb{Q}$.

Also, in [Cre2] it is conjectured that, over any quadratic imaginary number field, an elliptic curve of prime conductor $\mathfrak{p}$ exists only when there is a weight 2 newform, in the space of cuspidal automorphic forms for $\Gamma_0(\mathfrak{p})$, with certain properties.

In Chapter 2 we review some fundamental concepts of elliptic curves that will be needed chapters on elliptic curves following it. In Chapter 3 we give some fundamental facts concerning ramification in the prime division fields of elliptic curves, over p-adic fields, with multiplicative reduction. Chapter 4 deals with elliptic curves over the 9 quadratic number fields in question. I In Chapter 5 we gives results concerning the 3-division field. In particular, with the 3-division field we obtain results that parallel the type in [B-K]. These results, along with some in [Shu], yield the primes for our non-existence results. Chapter 5 is used to discuss them, as well as cases when you do have an existence result.

The second project studies an integer-valued invariant $g(M)$, called the g-integer of an arithmetical graph (G, M, R). Arithmetical graphs are interesting combinatorial objects and from a more abstract realm of degenerating an arithmetical algebraic curve. One naturally may seek to relate this invariant to other invariants of the arithmetical graph. Two important invariants of an arithmetical graph are its linear rank $g_0(M)$, which is integer-valued, and its component group $\Phi(M)$, which is a finite Abelian group. It is shown in [Lor2] that $g(M)$ is always bounded above by $g_0(M)$. There are other significant relationship between two of these invariants. For a positive integer $x = p_1^{a_i} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$ let $\ell(x) := \sum_{i=1}^{k} a_i \cdot (p_i - 1)$.

In [Lor3] it is shown that for an arithmetical tree

$$\ell(\#\Phi(M)) \leq 2g_0(M)$$

and that as a corollary

$$\#\Phi(M) \leq 4^{g_0(M)}.$$

As $g(M) \leq g_0(M)$ one may then try to see whether these two inequalities hold when $g_0(M)$ is replaced by $g(M)$. We address this question in Chapter 13 where we show by example that the first inequality fails. We also discuss why the second may hold in general, with evidence given to that end. Namely, we show that this inequality holds whenever either the g-integer is 1 or the tree has only 3 branches.

In Chapter 7 we consider the concept of gluing two arithmetical graphs together and are able to show that the change in g-integer is partially the same as the change in the linear rank. We give examples to show that, however, it does not always behave exactly the same. In Chapter 8 we look at the operation of blowing up an arithmetical graph and prove that this new invariant in unchanged after such an operation. In Chapters 9 and 10 we then shift our focus to arithmetical trees having g-integer at most 1. We are able to construct two families of arithmetical graphs where $g_0(M) \to \infty$, while $g(M)$ is always 0 (resp. 1) in the first (resp. second). Also, we give a nice complete description of a certain class of g-integer 1 arithmetical trees.

Another direction of study of this invariant is motivated by the fact that there is always a canonical divisor for $g_0(M)$ (see [Lor2]); that is, a degree $2g_0(M) - 2$ divisor K acting on the degree $g_0(M) - 1$ divisors by $D \mapsto K - D$, so that D is equivalent to an effective divisor precisely when $K - D$ is. It is natural to then ask whether there is a degree $2g(M) - 2$ divisor that acts analogously on degree $g(M) - 1$ divisors. We show with an example that on one

hand there is not always such a canonical divisor, and on the other hand there is sometimes more than one such divisor.

Finally, it is advantageous to be able to compute this invariant on your favorite example. Appendix B and Appendix C furnish this ability through programs written in the python language and used in the SAGE interface. In some cases one may hope to compute by hand a general formula for $g(M)$ in a family of examples. In Chapter 12 we do exactly this for the arithmetical graphs associated to the modular curves $X_0(p^2)$.

Chapter 2

Introduction to elliptic curves and number fields

We star by reviewing some basic notions of elliptic curves. Let K be a finite field extension of either $\mathbb{Q}_p$ (for some prime p) or $\mathbb{Q}$. Let $\mathcal{O}_K$ be its ring of integers. Let E/K be an elliptic curve defined over K. At a (non-zero) prime ideal $\mathfrak{P}$ our elliptic curve E will have either good, multiplicative, or additive reduction (see 3.6 in [Ade]). It turns out that the reduction is good at all but finitely many such primes.

There is an ideal in $\mathcal{O}_K$, called the conductor of E/K, that catalogs the bad (i.e., multiplicative or additive) reduction (see pg. 388 in [Sil1]). The primes that divide the conductor are precisely the primes of bad reduction. Moreover, E/K has additive reduction at $\mathfrak{P}$ if and only if $\mathfrak{P}^2$ divides the conductor. We will say that E/K has semi-stable reduction at $\mathfrak{P}$ if the reduction is either good or multiplicative. If the reduction is semi-stable at every prime then we say E/K has everywhere semi-stable reduction. Thus, E/K has everywhere semi-stable reduction if and only if the conductor is square-free.

Let ℓ be a prime number. The points of order dividing ℓ on E that are defined over $\overline{K}$ are denoted by $E[\ell]$. For a fixed Weierstrass equation of E/K we let $K(E[\ell])$ denote the field extension of K gotten by adjoining the coordinates of all points of $E[\ell]$ to K. It turns out that this finite extension is Galois and independent of the chosen Weierstrass equation for E/K.

It is shown that $E[\ell]$ admits the structure of a two dimensional $\mathbb{F}_\ell$ vector space (see 3.4 in [Ade]). We fix an $\mathbb{F}_\ell$ ordered basis on $E[\ell]$ and hence identify $\mathrm{End}_{\mathbb{F}_\ell}(E[\ell])$ with $\mathrm{GL}_2(\mathbb{F}_\ell)$. Also, the natural action of $\mathrm{Gal}(K(E[\ell]/K)$ on $E[\ell]$ is by $\mathbb{F}_\ell$ linear endomorphisms. Consequently, we then have the associated group homomorphism

$$\rho : \mathrm{Gal}(K(E[\ell])/K) \to \mathrm{GL}_2(\mathbb{F}_\ell).$$

It is a fact that ρ is injective (see 3.4 in [Ade]).

Suppose that K now denotes a number field. We review class field theory, some of which will be used in the sequel. A *modulus* is a formal finite product of positive integral powers of

primes (including the infinite ones) of K, $\mathfrak{c} = \prod \mathfrak{p}^{m(\mathfrak{p})}$, where for any infinite prime $m(\mathfrak{p}) \leq 1$. We then have $I(\mathfrak{c})$, the group generated by all ideals of K not in the support of $\mathfrak{c}$. For a finite prime $\mathfrak{p}$ let $\mathfrak{o}_\mathfrak{p}$ be the associated local ring and $\mathfrak{p}_v$ its maximal ideal. One checks that $I(\mathfrak{c})$ contains the following subgroup:

$$P_\mathfrak{c} := \{(\alpha) \text{ fractional ideal of } K : \text{if } \mathfrak{p}|\mathfrak{c} \text{ is finite then } \alpha \in \mathfrak{o}_\mathfrak{p} \text{ and } \alpha\text{-}1 \in \mathfrak{p}_v^{m(\mathfrak{p})}, \text{ while if } \sigma_v = \mathfrak{p}|\mathfrak{c} \text{ is infinite then } \sigma_\mathfrak{p}(\alpha) > 0\}.$$

The finite quotient group $I(\mathfrak{c})/P_\mathfrak{c}$ is called the *ray class group* of K with respect to (the modulus) $\mathfrak{c}$. Its order is called the *ray class number*.

Suppose now that L is a finite Abelian extension of K. If it is the case that the support of $\mathfrak{c}$ contains all the primes of K that ramify in L then we have the *Artin map*

$$\omega : I(\mathfrak{c}) \to \mathrm{Gal}(L/K)$$

This group homomorphism is defined by sending a prime ideal of K to its Frobenius automorphism with respect to L. It can be shown that the Artin map is always surjective (see Theorem 1 in X of [Lan]).

Put $\mathfrak{N}_K^L(\mathfrak{c})$:=group of norms of fractional ideals of L that lie above no prime in $\mathfrak{c}$. It turns out that $\mathfrak{N}_K^L(\mathfrak{c})$ is always in $ker(\omega)$. Further, there is a particular modulus of K, called the *conductor* of L/K (see 3.4.1 in [Coh]) and denoted by $\mathfrak{f}(L/K)$. It turns out that the primes that divide the conductor are precisely the primes of K that ramify in L. Moreover, we have that $P_{\mathfrak{f}(L/K)}$ is in $\ker(\omega)$. In this case it can be shown that $\ker(\omega) = P_\mathfrak{c}\mathfrak{N}_F^L(\mathfrak{c})$.

Chapter 3

Properties of the ℓ-th division fields: the local case

For all of this chapter, unless otherwise stated, we take up each of the following conventions. Let K be a finite extension of $\mathbb{Q}_p$ for some fixed prime p. Let $\mathcal{O}_K$ denote its ring of integers with $\mathfrak{M} = (\pi)$ the non-units and $k := \mathcal{O}_K/\mathfrak{M}$ the associated residue field. Let ℓ be any fixed prime. Suppose that E/K is an elliptic curve with multiplicative reduction. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be any fixed minimal Weierstrass equation for E/K. Denote by Δ, c_4, and c_6 the usual quantities for this equation. Finally, $|\cdot|$ represents the (π)-adic absolute value on K.

As E has multiplicative reduction over K and our Weierstrass equation is minimal we must have (see Proposition VII.5.1(b) in [Sil2]) that $c_4 \in \mathcal{O}_K^*$. Since $c_4^3 - c_6^2 = 1728\Delta$ we then get c_6 is also in $\mathcal{O}_K^*$.

3.1. Since E has multiplicative reduction over K we know $|j(E)| > 1$, so we can apply the theory of Tate curves (see Theorem V.5.3 in [Sil1]). This says there is a unique non-zero element q of $\mathcal{O}_K$ such that E is isomorphic over $K(\sqrt{-c_6})$ to the Tate curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n},\ a_4(q) = -5s_3(q), \text{ and } a_6(q) = \tfrac{5s_3(q)+7s_5(q)}{-12}.$$

We then get its discriminant being $\Delta_q = q\prod_{n\geq 1}(1-q^n)^{24}$.

Also, let $q^{\frac{1}{\ell}}$ be any fixed ℓ-th root of q in 3.1 and let ζ_ℓ be any fixed primitive ℓ-th root of unity. Let $E[\ell]$ be the points of order E defined over $\overline{K}$ that have order diving ℓ (see Chapter 1). Finally, denote by L the ℓ-th division field of E; that is, $L := K(E[\ell])$.

Lemma 3.2. *We have* $K(\sqrt{-c_6})(E[\ell]) = K(\sqrt{-c_6}, \zeta_\ell, q^{\frac{1}{\ell}})$.

Proof : As E and E_q (see 3.1) are isomorphic over $K(\sqrt{-c_6})$ we immediately get $K(\sqrt{-c_6})(E[\ell]) = K(\sqrt{-c_6})(E_q[\ell])$. Since $K(\sqrt{-c_6})(E_q[\ell])$ is the smallest extension of $K(\sqrt{-c_6})$ where E_q attains all its ℓ-torsion we have (see Theorem V.3.1(d) in [Sil1]) that

$$K(\sqrt{-c_6})(E[\ell]) = K(\sqrt{-c_6}, \zeta_\ell, q^{\frac{1}{\ell}}).$$

Indeed, the ℓ-torsion subgroup of $\overline{K}^*/q^{\mathbb{Z}}$ is generated by $\{[\zeta_\ell], [q^{\frac{1}{\ell}}]\}$. □

Corollary 3.3. *Suppose ℓ is odd. Then $K(E[\ell]) = K(\sqrt{-c_6}, \zeta_\ell, q^{\frac{1}{\ell}})$.*

Proof : We show for $L := K(E[\ell])$ that E_L/L does not have non-split multiplicative reduction (and so it will have split multiplicative reduction). This will give (by Theorem V.5.3 in [Sil1]) that $\sqrt{-c_6} \in L$, and hence (by Lemma 3.2) our desired conclusion.

Suppose the reduction is non-split. Then, $[E(L) : E_0(L)] \leq 2$ (Remark 2.2.4 in [Liu]). Thus as ℓ is odd we get $E[\ell] \subset E_0(L)$.

Let k_0 be the residue field for L. Now $E_0(L)/E_1(L) \cong \widetilde{E}_{ns}(k_0)$. Since the reduction is multiplicative we know $\#\widetilde{E}_{ns}(k_0)$ (is finite and) not a multiple of p.

Thus, if $\ell = p$ then $E[\ell]$ is actually in $E_1(L)$. But then $E_1(L)$ has a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$, contradicting E_L/L having multiplicative reduction (see Exercise 4.4 in [Sil2]).

If $\ell \neq p$ then $E_1(L)$ has no non-zero ℓ-torsion (Proposition 3.1(a) in [Sil2]), so $E[\ell]$ embeds in $\widetilde{E}_{ns}(k_0)$ implying that $\widetilde{E}_{ns}(k_0)$ is non-cyclic. But then E_L/L cannot have bad reduction, a contradiction. □

Remark 3.4. Note that this corollary cannot be extended to the case $\ell = 2$. Indeed, $E/\mathbb{Q}$ given by $y^2 + xy + x^2 = x^3 - 19x + 26$ (this is curve 30A2 in [Cre1]) has conductor 30, $c_6 = -24013$ and $\mathbb{Q}_2(E[2]) = \mathbb{Q}_2$ while $\sqrt{-c_6} \notin \mathbb{Q}_2$. Also, $E/\mathbb{Q}$ given by $y^2 + xy + x^2 = x^3 + x^2 - 135x - 660$ (this is curve 15A2 in [Cre1]) has conductor 15, $c_6 = 521479$, and $\mathbb{Q}_3(E[2]) = \mathbb{Q}_3$ while $\sqrt{-c_6} \notin \mathbb{Q}_3$. These examples also tell us that the first part of Proposition 5.1.3 in [B-K] is not true as stated.

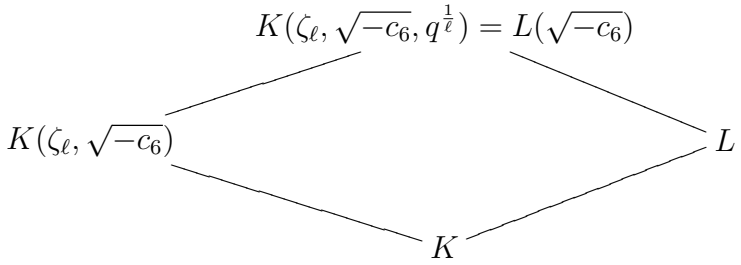
Lemma 3.5. *It holds that $ord_{(\pi)}(\Delta) = ord_{(\pi)}(q)$.*

Proof : We see that $\mathrm{ord}_{(\pi)}(q) = \mathrm{ord}_{(\pi)}(\Delta_q)$ by 3.1, due to the fact that a sequence of elements of $\mathcal{O}_K^*$ can converge in $\mathcal{O}_K$ to only an element of $\mathcal{O}_K^*$. Now $-\mathrm{ord}_{(\pi)}(j(E_q)) = \mathrm{ord}_{(\pi)}(\Delta_q)$. Then, since $j(E) = j(E_q)$, all we have to now show is that $\mathrm{ord}_{(\pi)}(j(E)) = \mathrm{ord}_{(\pi)}(\Delta)$. As $j(E) = \frac{c_4^3}{\Delta}$, and (by 3.1) $c_4 \in \mathcal{O}_K^*$, we have what we want. □

Theorem 3.6. *Let e denote the ramification index of L/K. Suppose $\ell \neq p$. Then*

$$e = \begin{cases} \ell & \text{if } ord_{(\pi)}(\Delta) \not\equiv 0 \ (mod\ \ell) \\ 1 & \text{otherwise} \end{cases}$$

Proof : We have the following diagram:



First, observe that $K(\zeta_\ell, \sqrt{-c_6})/K$ is unramified. Put, as we can, $q = u\pi^s$ where $s \in \mathbb{N} \cup \{0\}$ and $u \in \mathcal{O}_K^*$. Thus s=ord$_{(\pi)}(\Delta)$ by Lemma 3.5. If $s \equiv 0 \ (mod\ \ell)$ then $K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}})$ arises by taking $K(\zeta_\ell, \sqrt{-c_6})$ and adjoining to it any fixed ℓ-th root of u. Thus, in this case $K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}})/K(\zeta_\ell, \sqrt{-c_6})$ is unramified (see [Bir] pg. 91 Lemma 5). If $s \not\equiv 0 \ (mod\ \ell)$ then we have some $t \in \mathbb{N}$ with $t < \ell$ such that we get $K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}})$ from $K(\zeta_\ell, \sqrt{-c_6})$ by adjoining any fixed ℓ-th root of $u\pi^t$. But then, as π is still a uniformizer in $K(\zeta_\ell, \sqrt{-c_6})$ by the unramifiedness of $K(\zeta_\ell, \sqrt{-c_6})/K$, the extension $K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}})/K(\zeta_\ell, \sqrt{-c_6})$ is ramified ([Bir] pg. 92 Lemma 6). As $[K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}}) : K(\zeta_\ell, \sqrt{-c_6})] = \ell$ in this case (due to $K(\zeta_\ell, \sqrt{-c_6})$ containing μ_ℓ) it follows that the ramification index of $K(\zeta_\ell, \sqrt{-c_6}, q^{\frac{1}{\ell}})/K(\zeta_\ell, \sqrt{-c_6})$ is ℓ.

From all this we can deduce the value of e introduced above. Since, $L(\sqrt{-c_6})/L$ is unramified unramified we know that the ramification index of L/K equals the ramification index of $L(\sqrt{-c_6})/K$, which is e. □

Corollary 3.7. *Let K be a number field. Suppose that E/K is an elliptic curve with multiplicative reduction at a prime $\mathfrak{P}$. Let ℓ be any prime not contained in $\mathfrak{P}$. Let Δ be the discriminant of any fixed integral Weierstrass equation for E/K that is minimal at $\mathfrak{P}$. Let K_v denote the completion of K with respect to the $\mathfrak{P}$-adic absolute value. Let π be a uniformizer for $\mathcal{O}_{K_v}$. Then, the ramification index, e, of $\mathfrak{P}$ in $F := K(E[\ell])$, is as in the Theorem 3.5:*

$$e = \begin{cases} \ell & \text{if } ord_{(\pi)}(\Delta) \not\equiv 0 \ (mod\ \ell) \\ 1 & \text{otherwise} \end{cases}$$

Proof : Let $\mathfrak{Q}$ be any fixed prime of F above $\mathfrak{P}$. Here F_w denotes the completion of F with respect to the $\mathfrak{Q}$-adic absolute value. Embed F and K_v (and hence $K_v(E[\ell])$) into F_w. The ramification index of $\mathfrak{P}$ in F equals the ramification index for the extension F_w/K_v. Since $F_w = K_v{\cdot}F = K_v(E[\ell])$ we are done in light of the Theorem 3.6. □

Proposition 3.8. *Suppose that $\ell = p$ and also that $ord_{(\pi)}(q) \not\equiv 0$ (mod ℓ). Then L/K is wildly ramified.*

Proof : Since $\mathrm{ord}_{(\pi)}(q) \not\equiv 0$ (*mod* ℓ) there exists $s \in \mathbb{N}$ and $u \in \mathcal{O}_K^*$ with $s < \ell$ such that for an appropriate an appropriate fixed choice of ℓ-th root of $u\pi^s$, which we denote by $\sqrt[\ell]{u\pi^s}$, we have

$$K(q^{\frac{1}{\ell}}) = K(\sqrt[\ell]{u\pi^s}).$$

Suppose $\sqrt[\ell]{u\pi^s} \in K(\zeta_\ell)$. Let π_0 be any fixed choice of uniformizer for $\mathcal{O}_{K(\sqrt[\ell]{u\pi^s})}$ and t_0 be the ramification index for $K(\sqrt[\ell]{u\pi^s})/K$. Then, as $[K(\zeta_\ell) : K] \mid (\ell - 1)$, we have $st_0 = \ell{\cdot}\mathrm{ord}_{(\pi_0)}(\sqrt[\ell]{u\pi^s})$ and $t_0 \leq \ell - 1$. Thus $\ell \mid st_0$, contradicting that $s, t_0 < \ell$.

Consequently, $\sqrt[\ell]{u\pi^s} \notin K(\zeta_\ell)$ must hold so $[K(\zeta_\ell, \sqrt[\ell]{u\pi^s}) : K(\zeta_\ell)] = \ell$. Thus,

$$\ell \mid [K(\zeta_\ell, \sqrt[\ell]{u\pi^s}) : K(\sqrt[\ell]{u\pi^s})] \cdot [K(\sqrt[\ell]{u\pi^s}) : K].$$

Then, since $[K(\zeta_\ell, \sqrt[\ell]{u\pi^s}) : K(\sqrt[\ell]{u\pi^s})] \mid (\ell - 1)$ we know that $\ell = [K(\sqrt[\ell]{u\pi^s}) : K]$. Finally, we see that $K(\sqrt[\ell]{u\pi^s})/K$ is ramified, and hence, by what we just showed, totally ramified.

Therefore, ℓ divides the ramification index for $K(\zeta_\ell, q^{\frac{1}{\ell}}, \sqrt{-c_6})/K$, so, by 3.2, ℓ divides the ramification index for $K(E[\ell], \sqrt{-c_6})/K$. Then, since $K(E[\ell], \sqrt{-c_6})/K(E[\ell])$ is always unramified, we are done with the proof. □

While the following proposition is not used in the rest of this article we offer it because it shows how easy it is, in certain cases, to compute all the higher ramification groups of L/K.

Put $G :=\mathrm{Gal}(L/K)$ and $G_K :=\mathrm{Gal}(\overline{K}/K)$. For each F/K finite Galois we have on one hand for each real number $u \geq -1$ the upper numbered higher ramification group $\mathrm{Gal}(F/K)^u$ and on the other hand for each integer $u \geq -1$ the lower numbered higher ramification group $\mathrm{Gal}(F/K)_u$ (as in 4.1 and 4.3 of [Ser1]). We then define G_K^u as the (necessarily closed) subgroup of G_K that gets identified with $\varprojlim \mathrm{Gal}(F/K)^u$ when we identify G_K with our usual profinite group (here, as expected, the inverse limit is taken over all finite Galois extensions of K that are contained in $\overline{K}$).

Lemma 3.9. *The restriction homomorphism ($G_K \to G$) takes G_K^u (into and) onto G^u.*

Proof : If the image were smaller than G^u then G_K^u operates trivially on an element, say α, of $L - L^{G^u}$. But, by Proposition 3.9 in [Kaw], we know $\overline{K}^{G_K^u} = \bigcup F^{Gal(F/K)^u}$, where the union is taken over all F/K finite Galois, and so $K(\alpha) \subset F^{Gal(F/K)^u}$ for some F/K finite Galois. But, by Theorem 2.A(II) in [Kaw], $L^{G^u} \bigcap K(\alpha) = K(\alpha)^{Gal(K(\alpha)/K)^u}$. Then, since $K(\alpha) = K(\alpha)^{Gal(K(\alpha)/K)^u}$, due to the fact that $F^{Gal(F/K)^u} \bigcap K(\alpha) = K(\alpha)^{Gal(K(\alpha)/K)^u}$, we therefore get $K(\alpha) \subset L^{G^u}$, a contradiction.

Proposition 3.10. *Suppose $K/\mathbb{Q}_p$ is unramified, $\ell = p$, and L/K is wildly ramified. Then $\#G_1 = p$ and $\#G_u = 1$ for $u > 1$ in $\mathbb{Z}$.*

Proof : As $K/\mathbb{Q}_p$ is unramified we can invoke the Corollaire on pg. 277 in [Ser2], giving that either $\#G_0 = p^2 - p$ or $\#G_0 = p - 1$ holds. By the existence of wild ramification we know that the former holds and also that $\#G_1 = p$. Suppose $\#G_2 \neq 1$ (so $\#G_2 = p$). Thus, $G_2 = G^{\frac{2}{p-1}}$. But Lemma 3.9 then gives that $L \nsubseteq \overline{K}^{G_K^{\frac{2}{p-1}}}$; that is, $G_K^{\frac{2}{p-1}}$ acts non-trivially on $E[p]$. This contradicts Theorem A in [Fon].

Remark 3.11. This proposition yields, among other things, a more immediate proof of Lemma 3.3.2 in [Klu].

Remark 3.12. The conclusion of Proposition 3.10 holds also, as the proof showed, when the suppositions are the same except that E/K has good (instead of multiplicative) reduction.

Before we proceed let us introduce the following notation.

Let I denote the inertia group of L/K and put again $G :=\mathrm{Gal}(L/K)$ and $I_p :=\mathrm{Gal}(\overline{K}/K_{tr})$. Here K_{tr} denotes the compositum of all finite at worst tamely ramified extensions of K (thus K_{tr} contains no finite wildly ramified extension of K). Let $\rho : G \to GL_2(\mathbb{F}_p)$ be any fixed group homomorphism arising from the usual G-module structure of $E[p]$ (see Chapter 1). Note that ρ is injective.

For the next theorem we make use of the facts that restricting elements of $I(\overline{K}/K)$ to G yields the subgroup I and restricting elements of $\mathrm{Gal}(\overline{K}/K))$ to G gives all of G itself. Also, we note that the field fixed by all elements of I_p is K_{tr}.

Theorem 3.13. *Suppose that $K/\mathbb{Q}_p$ is unramified and $\ell = p$. Then the following are both true:*

(a) *If* $ord_{(\pi)}(\Delta) \not\equiv 0 \ (mod\ \ell)$ *then* $\rho(I)$ *is conjugate to* $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ *(so* $\#\rho(I) = \ell(\ell-1)$*).*

(b) *If* $ord_{(\pi)}(\Delta) \equiv 0 \ (mod\ \ell)$ *then* $\rho(I)$ *is conjugate to* $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ *(so* $\rho(I)$ *is cyclic of order* $\ell-1$*), or* $\rho(I)$ *is conjugate to* $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

Proof :

(a) By the Corollary(c) on pg. 277 of [Ser2] we see that we are done in light of Proposition 1.7.

(b) Since either (b) or (c) of the Corollary on pg. 277 of [Ser2] holds we clearly have what is claimed. Further, we can use the corollary to figure out which occurs. □

Remark 3.14. It should be noted that in Theorem 3.13 it is possible to have an example of an unramified p-adic field K and an elliptic curve E/K of multiplicative reduction such that $\text{ord}_{(\pi)}(\Delta) \equiv 0 \ (mod\ p)$ and at the same time have $\rho(I)$ be as in (a). For an example start with $E/\mathbb{Q}$ given by $y^2 + xy = x^3 - x^2 - x + 1$ (this is curve 58A1 in [Cre1]), which has $\Delta = -116$ and conductor 58. Take this curve over $K := \mathbb{Q}_2$ with $\ell = p = 2$ and π a uniformizer of $\mathbb{Z}_2$. We then have $\text{ord}_{(\pi)}(\Delta) = 2$, but $\sqrt{-29} \in \mathbb{Q}_2(E[2])$ while $\mathbb{Q}_2(\sqrt{-29})/\mathbb{Q}_2$ is ramified. Hence $\#I = \#\rho(I)$ is not $\ell - 1$. This example also shows that Proposition 5.1.3.d in [B-K] is not true as stated.

Theorem 3.15. *Suppose that* E/K *is an elliptic curve with good reduction (keep all other notation as before),* $K/\mathbb{Q}_p$ *is unramified, and* $\ell = p$.

(a) *If the reduction is ordinary then*

$$\rho(G) \text{ is conjugate to a subgroup of } \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \text{ (so } \#\rho(G) \mid \ell(\ell-1)^2) \tag{3.1}$$

$$\rho(I) \text{ is conjugate to } \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \text{ or is conjugate to } \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.2}$$

(b) *If the reduction is supersingular then*

$$\rho(I) \text{ is cyclic of order } \ell^2 - 1 \tag{3.3}$$

$$\rho(G) = \rho(I) \text{ if } 2 \mid [k : \mathbb{F}_\ell] \tag{3.4}$$

$$[\rho(G) : \rho(I)] = 2 \text{ with } \rho(G) \text{ the normalizer of } \rho(I) \text{ in } GL_2(\mathbb{F}_\ell) \text{ if } 2 \nmid [k : \mathbb{F}_\ell] \tag{3.5}$$

Proof : The first part follows from a comment on pg. 273 of [Ser2] along with the Corollary on pg. 274 of [Ser2]. The second part is a result of Proposition 12 on pg. 275 of [Ser2] (along with a comment made in the first paragraph of Section 2.2. on pg. 279 of [Ser2]). □

We then have the following corollaries to Theorem 3.13 and Theorem 3.15.

Corollary 3.16. *Let K be a number field and E/K an elliptic curve. Let Δ be the discriminant of any fixed integral Weierstrass equation for E/K that is minimal at a prime $\mathfrak{P}$. Suppose that E/K has multiplicative reduction at $\mathfrak{P}$ and that $\mathfrak{P}$ is unramified over the prime number ℓ that is below it. Let K_v denote the completion of K with respect to the $\mathfrak{P}$-adic absolute value. Let π be a uniformizer for $\mathcal{O}_{K_v}$. Let I be an inertia subgroup of $\mathfrak{P}$ in $K(E[\ell])$. Then the conjugacy class of our $\rho(I)$ is the same as the conjugacy class of the $\rho(I)$ in Thm 3.13.*

Corollary 3.17. *Let K be a number field and E/K an elliptic curve. Suppose that E/K has good reduction at $\mathfrak{P}$ and that $\mathfrak{P}$ is unramified over the prime number ℓ below it. Let K_v denote the completion of K with respect to the $\mathfrak{P}$-adic absolute value. Let I (resp. D) be an inertia (resp. decomposition) subgroup of $\mathfrak{P}$ in $K(E[\ell])$. In the conclusion of Theorem 3.15 replace $\rho(G)$ (resp. $\rho(I)$) by our $\rho(D)$ (resp. our $\rho(I)$) here and use our $\mathcal{O}_K/\mathfrak{P}$ here in place of k. Then our $\rho(I)$ and $\rho(D)$ satisfy all properties stated in the conclusion of Theorem 3.15.*

Chapter 4

Properties of the 3-division field: the number field case

We will let K denote a number field and E/K an elliptic curve. Throughout this chapter Δ will be the discriminant of a Weierstrass equation for E/K. We denote by $\Delta^{\frac{1}{3}}$ an arbitrary but fixed cube root of Δ.

We will investigate $K(E[3])$, the 3-division field of E/K. This is a Galois extension of K and $\#\mathrm{Gal}(K(E[3])/K)$ divides 48 (see 3.4 in [Ade]). Let $f(x) \in K[x]$ be any fixed 3rd-division polynomial of E/K. Recall that f is a separable quartic whose roots in $\overline{K}$ are precisely the x-coordinates that occur for $P \neq 0$ in $E(\overline{K})[3]$.

4.1. We have the following facts:

(a) The splitting field of f over K, denoted by K_f, is contained in $K(E[3])$

(b) $[K(E[3]) : K_f] \leq 2$

(c) $K(\zeta_3, \Delta^{\frac{1}{3}})$ is the splitting field of the cubic resolvent of f (so in particular it is contained in K_f).

For (b) and (c) see, respectively, Prop 5.2.2(c) and Proposition 5.4.3 of [Ade].

Lemma 4.2. *We have $\Delta \in K^{*3}$ if and only if $3 \nmid [K(E[3]) : K]$.*

Proof : For the if implication use 4.1(c) and 4.1(a). We have the only if part by (b) and (c) in 4.1, along with the fact that the degree of K_f over the splitting field of its cubic resolvent divides 4 (see Proposition 5.4.3 in [Ade]). □

Proposition 4.3. *Suppose that E/K has everywhere semi-stable reduction. Then a finite prime $\mathfrak{P}$ of $K(\Delta^{\frac{1}{3}})$ will ramify in $K(E[3])$ only if $3 \in \mathfrak{P}$.*

Proof : Put $F := K(\Delta^{\frac{1}{3}})$. We know that E_F/F is semi-stable, as well. Let $\mathfrak{P}$ be prime of $\mathcal{O}_F$ with $3 \notin \mathfrak{P}$. If E_F/F has good reduction at $\mathfrak{P}$ then $\mathfrak{P}$ is unramified since, by the Néron-Ogg-Shafarevich Criterion (see Theorem VII.7.1 in [Sil2]), it is unramified locally. If, however, E_F/F has multiplicative reduction at $\mathfrak{P}$ then we use Corollary 3.7 applied to the number field F, yielding that if $\mathfrak{P}$ is ramified in $K(E[3])$ then the ramification index is 3, so $3 \mid [K(E[3]) : F]$. But then by Lemma 4.2 we know $\Delta \notin K^{*3}$, making $3 \mid [F : K]$. Since $9 \nmid [K(E[3]) : K]$ we then have that $\mathfrak{P}$ does not ramify in $K(E[3])$. Therefore we are finished. □

Proposition 4.4. *Suppose $K \neq \mathbb{Q}(\zeta_3)$ is quadratic imaginary of class number 1, and that E/K has everywhere semi-stable reduction. Suppose further that E/K has no K-rational three isogeny. Then $\Delta \notin K^{*3}$ and $\#Gal(K(E[3])/K) = 48$.*

Proof : Suppose $\Delta \in K^{*3}$. Since $\zeta_3 \notin K$ and E/K admits no K-rational three-isogeny we have by Lemma 10(2) and 10(3) in [Kag] that $\mathrm{Gal}(K(E[3])/K(\zeta_3))$ is isomorphic to either Q_8, the quaternion group of order 8, or $\mathbb{Z}/4\mathbb{Z}$. As every subgroup of Q_8 is normal (see Example 2.30 in [Rot]) we see that Q_8 must have an order 4 quotient. Thus, in either case above we see that $K(E[3])/K(\zeta_3)$ has a quartic Abelian sub-extension, say $K'/K(\zeta_3)$. Now as $\Delta \in K^{*3}$ we see that adjoining ζ_3 to K is the same as adjoining an appropriate cube root of Δ to K. Thus we can write $K(\zeta_3) = K(\Delta^{\frac{1}{3}})$. Then, by Proposition 4.3 we see that $K'/K(\zeta_3)$ is ramified only possibly at primes lying above (3). Consequently, ([Shu] last paragraph before 2.9) the $h_{(3)}(K(\zeta_3))$, the ray class number of $K(\zeta_3)$ with respect to the (integral ideal) modulus (3), must be divisible by 4 (see Chapter 2 for background on class field theory). But, $4 \nmid h_{(3)}(K(\zeta_3))$ (see the table on pg. 31 in [Shu]), a contradiction. Therefore, $\Delta \notin K^{*3}$.

Since E/K admits no K-rational three-isogeny we find by Lemma 10(3) from [Kag] that $\#\mathrm{Gal}(K(E[3])/K)$ is $\{8, 16, 48\}$. Since $\Delta \notin K^{*3}$ and Lemma 4.2 together tell us that $\#\mathrm{Gal}(K(E[3])/K)$ is a multiple of 3, we conclude that $\#\mathrm{Gal}(K(E[3])/K) = 48$. □

Proposition 4.5. *Suppose that $K \neq \mathbb{Q}(\zeta_3)$ is quadratic imaginary of class number 1, and E/K has prime conductor (π). Further, suppose that E/K has no K-rational three-isogeny. Then all of the following hold:*

(a) $ord_{(\pi)}(\Delta) \not\equiv 0 (mod\ 3)$

(b) $K(\Delta^{\frac{1}{3}}) = K((u\pi^k)^{\frac{1}{3}})$ *for some $u \in \mathcal{O}_K^*$, some k in $\{1, 2\}$, and some cube root of $u\pi^k$ (so for any $u' \in \mathcal{O}_K^*$ and any cube root of u' we have $K(\Delta^{\frac{1}{3}}) \neq K(u'^{\frac{1}{3}})$).*

Proof :

(a) Let $\Delta^{'}$ denote the discriminant of any global minimal Weierstrass equation for E/K. We get, by E/K having conductor (π), that $\Delta^{'} = u\pi^k$ for some $u \in \mathcal{O}_K^*$ and $k \in \mathbb{N}$. As Proposition 4.4 applies to the discriminant of any Weierstrass equation for E/K, we see that $\Delta^{'} \notin K^{*3}$. Thus, 3=$[K(\Delta^{'\frac{1}{3}}) : K]$. Then, since $\mathcal{O}_K^* \subset K^{*3}$ we know $[K(v^{\frac{1}{3}}) : K] \leq 2$ for any $v \in \mathcal{O}_K^*$ and any choice of cube root of v. Thus, we see that indeed $k = \text{ord}_{(\pi)}(\Delta^{'}) \not\equiv 0 (mod\ 3)$. As $\Delta = b^{12} \cdot \Delta^{'}$ for some $b \in K^*$, we must have $\text{ord}_{(\pi)}(\Delta) \not\equiv 0 (mod\ 3)$, as well.

(b) This is immediate from (a) as $\Delta = b^{12} \cdot \Delta^{'}$ for some $b \in K^*$ implies that $K(\Delta^{\frac{1}{3}}) = K(\Delta^{'\frac{1}{3}})$ for an appropriate cube root of $\Delta^{'}$; that is, an appropriate cube root of $u\pi^k$, where $u \in \mathcal{O}_K^*$ and k is in $\mathbb{N}$. □

We recall that we have a group homomorphism (see Chapter 1):

$$\rho : \text{Gal}(K(E[3])/K) \rightarrow \text{GL}_2(\mathbb{F}_3).$$

As ρ is injective (see 3.4 in [Ade]) we can and do identify $\text{Gal}(K(E[3])/K)$ with its image under ρ.

4.6. In $\text{GL}_2(\mathbb{F}_3)$ we have the matrices

$$\sigma := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \tau := \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and } \gamma := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We have $\sigma^2 = 1, \tau^8 = 1$, and $\sigma\tau\sigma = \tau^3$ (see pg. 728 in [B-K]).

Remark 4.7. When ρ is surjective we see that $K(\Delta^{\frac{1}{3}})$ is the fixed field of a subgroup of $\text{GL}_2(\mathbb{F}_3)$ of order sixteen. But the order sixteen subgroups are precisely the $2-$Sylow subgroups. Hence they are all conjugate to one another. In particular, since$\# < \sigma, \tau >= 16$, we can assume without loss of generality that the fixed field of $< \sigma, \tau >$ acting on $K(E[3])$ will be $K(\Delta^{\frac{1}{3}})$.

Proposition 4.8. *Suppose $K \neq \mathbb{Q}(\zeta_3)$ is quadratic imaginary of class number 1 and that E/K has everywhere semi-stable reduction. Further, suppose E/K admits no K-rational three-isogeny. Let $\mathfrak{P}$ a prime of $\mathcal{O}_K$ lying above (3). If E has supersingular good reduction at $\mathfrak{P}$ then for any fixed $K(\Delta^{\frac{1}{3}})$ we have: $\mathfrak{P}$ factors in $K(\Delta^{\frac{1}{3}})$ as $\mathfrak{p}_1^2\mathfrak{p}_2$ where $\mathfrak{p}_1 \neq \mathfrak{p}_2$.*

Proof : We know $K(\Delta^{\frac{1}{3}})$ is a cubic extension of K by Proposition 4.4. Since 3 ramifies in $\mathbb{Q}(\zeta_3)$ but not in K we know $\mathfrak{P}$ ramifies in $K(\zeta_3)$. As $K(\Delta^{\frac{1}{3}}, \zeta_3)$ is the Galois closure of $K(\Delta^{\frac{1}{3}})/K$ and $\mathfrak{P}$ ramifies in $K(\Delta^{\frac{1}{3}}, \zeta_3)$, it follows that $\mathfrak{P}$ ramifies in $K(\Delta^{\frac{1}{3}})$. If $\mathfrak{P}$ were totally ramified in $K(\Delta^{\frac{1}{3}})$ then we would have contradicted Theorem 3.15 (b), which says, in particular, that the ramification index of $\mathfrak{P}$ in $K(E[3])$ is not a multiple of 3. Therefore, we are done. □

Proposition 4.9. *Suppose $K \neq \mathbb{Q}(\zeta_3)$ is quadratic imaginary of class number 1, and E/K has everywhere semi-stable reduction. Further, suppose that E/K admits no K-rational three-isogeny. If E has supersingular good reduction at no prime above 3 then $K(\Delta^{\frac{1}{3}})$ has even class number.*

Proof : To prove this one can use the idea and steps found in Proposition 5.6 of [B-K]. We can and do assume by Remark 4.7 that $\mathrm{Gal}(K(E[3])/K(\Delta^{\frac{1}{3}})) =< \sigma, \tau >$. Since $K(\Delta^{\frac{1}{3}})$ has no real archimedean prime, we get by Proposition 4.3 that $K(E[3])/K(\Delta^{\frac{1}{3}})$ is ramified only possibly at primes that contain 3. Let $\mathfrak{P}$ be a prime of $K(\Delta^{\frac{1}{3}})$ that contains 3. Suppose that $\mathfrak{P}$ ramifies in $K(E[3])$. Let $\mathfrak{Q}$ be the prime of K below $\mathfrak{P}$. Let $\mathfrak{q}$ be a prime of $K(E[3])$ lying above $\mathfrak{P}$. Thus, as 3 ramifies in $\mathbb{Q}(\zeta_3)$ but not in K, we know that $\mathfrak{Q}$ ramifies in $K(\zeta_3, \Delta^{\frac{1}{3}})$ with even ramification index. Then, since $K(\zeta_3, \Delta^{\frac{1}{3}})/K$ is the Galois closure of $K(\Delta^{\frac{1}{3}})/K$, we know that $\mathfrak{Q}$ ramifies in $K(\Delta^{\frac{1}{3}})$. Then, as $[K(\Delta^{\frac{1}{3}}) : K] = 3$ (by Proposition 4.4), $\mathfrak{Q}$ factors in $K(\Delta^{\frac{1}{3}})$ as $\mathfrak{P}^3$ or $\mathfrak{P} \cdot \mathfrak{P}'^2$ or $\mathfrak{P}^2 \cdot \mathfrak{P}'$.

Suppose that $\mathfrak{Q}$ factors as $\mathfrak{P}^2 \cdot \mathfrak{P}'$. As E/K has either multiplicative or ordinary good reduction at $\mathfrak{Q}$ and $\mathfrak{Q}$ is unramified over (3), we can and do apply either Corollary 3.16 or Corollary 3.17, which yield $\#I(\mathfrak{q}/\mathfrak{Q}) = 2$ or 6. If $\#I(\mathfrak{q}/\mathfrak{Q}) = 6$ then as $3 \nmid [K(E[3])/K(\Delta^{\frac{1}{3}})]$ we must have $\mathfrak{Q}$ totally ramified in $K(\Delta^{\frac{1}{3}})$, which it is not. Thus $\#I(\mathfrak{q}/\mathfrak{Q}) = 2$ must hold. But then, as $\mathfrak{P}$ is ramified over $\mathfrak{Q}$ in our case here it would follow that $\mathfrak{P}$ would not ramify in $K(E[3])$, contradicting our above supposition that $\mathfrak{P}$ ramifies in $K(E[3])$.

Thus, $\mathfrak{Q}$ factors as either $\mathfrak{P}^3$ or $\mathfrak{P} \cdot \mathfrak{P}'^2$. Since $\mathfrak{Q}$ ramifies in $K(\zeta_3, \Delta^{\frac{1}{3}})$ with even ramification index, it follows that $\mathfrak{P}$ ramifies in $K(\zeta_3, \Delta^{\frac{1}{3}})$ with ramification index 2.

Thus, as $\#I(\mathfrak{q}/\mathfrak{Q}) = 2$ or 6, by Corollary 3.16 and Corollary 3.17, which we just discussed, we see that $\#I(\mathfrak{q}/\mathfrak{P}) = 2$ (again $3 \nmid [K(E[3])/K(\Delta^{\frac{1}{3}})]$), say generated by η. As order(η)=2, we see that $\eta \notin \{\tau, \tau^3, \tau^5, \tau^7, \sigma\tau, \sigma\tau^3, \sigma\tau^5, \sigma\tau^7\}$, since no element in this set has order 2. But this set is precisely the complement of $< \sigma, \tau^2 >$ in $< \sigma, \tau >$. Consequently, $\eta \in < \sigma, \tau^2 >$.

We have now shown that if $\mathfrak{P}$ is *any* prime of $K(\Delta^{\frac{1}{3}})$ ramifying in $K(E[3])$ and $\mathfrak{q}$ is *any* prime of $K(E[3])$ lying above $\mathfrak{P}$ then $I(\mathfrak{q}/\mathfrak{P})$ will be in $< \sigma, \tau^2 >$. Let K_0 be the fixed field

of $< \sigma, \tau^2 >$ acting on $K(E[3])$. Thus, K_0 is contained in the inertia field for $\mathfrak{P}$ whenever $\mathfrak{P}$ ramifies in $K(E[3])$. Consequently, $K_0/K(\Delta^{\frac{1}{3}})$ is unramified and quadratic. But this tells us that the Hilbert class field of $K(\Delta^{\frac{1}{3}})$ is an finite Galois extension of even degree over $K(\Delta^{\frac{1}{3}})$. As the Galois group of this extension is isomorphic to the ideal class group of $K(\Delta^{\frac{1}{3}})$, our claim that $K(\Delta^{\frac{1}{3}})$ has even class number follows. □

Corollary 4.10. *Over* $\mathbb{Q}(\sqrt{-163})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 2, 3, 7, 29, 43, 53, 71, 97, 103, 131, 137, 151, 173, 197, 227, 239, 257, 263, 283, 307, 311, 317, 347, 367, 373, 379, 401, 419, 439, 479, 491, 499.
Over $\mathbb{Q}(\sqrt{-67})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 2, 7, 13, 17, 29, 31, 41, 47, 73, 103, 127, 131, 149, 167, 173, 193, 211, 223, 227, 239, 241, 257, 269, 277, 283, 293, 317, 349, 359, 367, 397, 421, 431, 439, 449, 457, 461, 479, 491.
Over $\mathbb{Q}(\sqrt{-43})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 3, 5, 7, 11, 13, 17, 29, 31, 41, 43, 47, 53, 59, 79, 83, 97,107, 109, 127, 139, 157, 173, 181, 193, 197, 227, 239, 241, 251, 263, 311, 313, 349, 353, 367, 379, 397, 401, 431, 439, 443, 461, 479, 487, 491.
Over $\mathbb{Q}(\sqrt{-19})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 2, 3, 5, 7, 11, 13, 17, 23, 29, 41, 43, 59, 83, 97, 101, 131, 139, 167, 173, 191, 193, 197, 199, 241, 257, 263, 271, 277, 283, 313, 317, 347, 349, 367, 389, 397, 401, 419, 439, 443, 461, 463, 467, 491, 499.
Over $\mathbb{Q}(\sqrt{-7})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 2, 3, 5, 7, 11, 23, 29, 31, 43, 53, 59, 67, 71, 79, 103, 107, 109, 127, 137, 149, 151, 157, 163, 173, 179, 193, 227, 233, 241, 257, 263, 277, 283, 311, 313, 317, 331, 359, 367, 373, 379, 389, 401, 421, 439, 443, 449, 457, 463, 479, 487, 491, 499.
Over $\mathbb{Q}(\sqrt{-1})$ *we have no elliptic curve of prime conductor* (π) *if* $p \in (\pi)$ *and* p *is one of the following:* 2, 3, 5, 7, 13, 17, 23, 31, 37, 41, 59, 61, 73, 89, 97, 101, 103, 109, 113, 149, 167, 173, 193, 227, 239, 241, 263, 269, 281, 283, 293, 311, 313, 337, 349, 353, 367, 373, 389, 397, 401, 409, 419, 421, 433, 439, 457, 461, 479, 491.

Proof : Let K be one of the six fields listed. Suppose E/K is an elliptic curve of prime conductor (π) with $p \in (\pi)$ and p among those primes listed for K. Then E/K admits no rational K-rational three-isogeny by [Shu] Proposition 2.15 if $p \neq 3$ and by Proposition 4.11 below if $p = 3$. Thus, by Proposition 4.5 (a) we see that $K(\Delta^{\frac{1}{3}}) = K((u\pi^k)^{\frac{1}{3}})$ for

some $u \in \mathcal{O}_K^*$ and some k in $\{1,2\}$. Then going through each possible choice of $u \in \mathcal{O}_K^*$ and $k \in \{1,2\}$ we use **PARI/GP** ([Pgp]) to perform two computations (see Appendix A). In fact, since $\mathcal{O}_K^* = \{1,-1\}$ and for each k in $\{1,2\}$ we have $K((\pi^k)^{\frac{1}{3}})$ isomorphic over K to $K((-\pi^k)^{\frac{1}{3}})$, we will only have to go through $K((\pi^k)^{\frac{1}{3}})$ for $k \in \{1,2\}$. We do indeed take advantage of this fact in our computations (see Appendix A). The first computation performed is the factorization of (3) in $K(\Delta^{\frac{1}{3}})$. The second is the class number of $K(\Delta^{\frac{1}{3}})$. The former yields that (3) factors in $K(\Delta^{\frac{1}{3}})$ with ramification index 3 and inertial degree 2. As 3 in inert in K this implies that (3), as a prime of K, factors in $K(\Delta^{\frac{1}{3}})$ as $\mathfrak{q}^3$. Thus Proposition 4.8 says that E does not have supersingular reduction at (3). The latter computation yields that $K(\Delta^{\frac{1}{3}})$ has odd class number, which, by Proposition 4.9 and the fact that 3 is inert in K, tells us that E must have supersingular reduction at (3). As the results of these computations are the same no matter what $k \in \{1,2\}$ we use we conclude that E/K cannot exist, as claimed. □

Proposition 4.11. *Let K be imaginary quadratic of class number 1 with 3 not splitting completely in K (let $\mathfrak{P}$ denote the unique prime above 3). If E/K is an elliptic curve having good reduction away from $\mathfrak{P}$, and potentially multiplicative reduction at $\mathfrak{P}$, then E/K admits no K-rational three-isogeny.*

Proof : If $K = \mathbb{Q}(\sqrt{-3})$ then we are done by the fact that in Table 2 in [Pin] it is shown that $j(E) \in \mathcal{O}_K$, making E/K have potentially good reduction everywhere. Thus we assume $K \neq \mathbb{Q}(\sqrt{-3})$. Suppose E/K does admit a K-rational three-isogeny, say to E'/K. Then by Theorem 1.2 in [Pin] there exist $\tau, \tau' \in K$ such that

(a) $\tau\tau' = 3^6$

(b) $j(E) = \frac{(\tau+27)(\tau+3)^3}{\tau}$

(c) $j(E') = \frac{(\tau'+27)(\tau'+3)^3}{\tau'}$.

Since K has class number 1, we know that every elliptic curve over K has a global minimal Weierstrass equation. First, let Δ and c_4 be the invariants of one (and hence every) global minimal Weierstrass equation for E/K. By (a) we know that either $\mathrm{ord}_{\mathfrak{P}}(\tau) > 0$ or $\mathrm{ord}_{\mathfrak{P}}(\tau') > 0$. Without loss of generality assume that $\mathrm{ord}_{\mathfrak{P}}(\tau) > 0$. Now since E has potentially multiplicative reduction at $\mathfrak{P}$ we have that $\mathrm{ord}_{\mathfrak{P}}(j(E)) < 0$, so $\mathrm{ord}_{\mathfrak{P}}(\tau+27) + 3\mathrm{ord}_{\mathfrak{P}}(\tau+3) < \mathrm{ord}_{\mathfrak{P}}(\tau)$. But as $\mathrm{ord}_{\mathfrak{P}}(\tau) > 0$ we already know that $\mathrm{ord}_{\mathfrak{P}}(\tau+27), \mathrm{ord}_{\mathfrak{P}}(\tau+3) >$

0. Thus, $\text{ord}_{\mathfrak{P}}(\tau) > 4$. Hence, $\text{ord}_{\mathfrak{P}}(\tau+27) \geq 3$. This makes $\text{ord}_{\mathfrak{P}}(\tau) > 6$ (and so $\text{ord}_{\mathfrak{P}}(\tau+3) = 2$). It also makes $\text{ord}_{\mathfrak{P}}(\tau+27) = 3$ (resp. $= 6$) if 3 is inert (resp. 3 ramifies). Hence, $\text{ord}_{\mathfrak{P}}(\tau) > 12$ if 3 ramifies. But then $\text{ord}_{\mathfrak{P}}(\Delta) = -\text{ord}_{\mathfrak{P}}(j(E)) + 3\text{ord}_{\mathfrak{P}}(c_4) = \text{ord}_{\mathfrak{P}}(\tau) - \text{ord}_{\mathfrak{P}}(\tau+27) - 3\text{ord}_{\mathfrak{P}}(\tau+3) + 3\text{ord}_{\mathfrak{P}}(c_4) = \text{ord}_{\mathfrak{P}}(\tau) - 6 + 3\text{ord}_{\mathfrak{P}}(c_4)$ (resp. $= \text{ord}_{\mathfrak{P}}(\tau) - 12 + 3\text{ord}_{\mathfrak{P}}(c_4)$) if 3 is inert (resp. if 3 ramifies).

Also, if $\mathfrak{P}' \neq \mathfrak{P}$ is a prime then $\text{ord}_{\mathfrak{P}'}(j(E)) \geq 0$ since E has good reduction at $\mathfrak{P}'$, making

$$0 \leq \text{ord}_{\mathfrak{P}'}(j(E)) = \text{ord}_{\mathfrak{P}'}(\tau+27) + 3\text{ord}_{\mathfrak{P}'}(\tau+3) - \text{ord}_{\mathfrak{P}'}(\tau).$$

If $\text{ord}_{\mathfrak{P}'}(\tau) < 0$ then the far right expression equals $3\text{ord}_{\mathfrak{P}'}(\tau)$, a contradiction. Thus $\text{ord}_{\mathfrak{P}'}(\tau') \geq 0$ since K-isogenous elliptic curves have the same conductors.

Suppose first that 3 is inert. Put $\Delta = 3^k u$ where $u \in \mathcal{O}_K^*$ and $k \in \mathbb{N}$. Also, we see that $\tau = 3^m v, \tau' = 3^{m'} v'$ where $v, v' \in \mathcal{O}_K$ are not divisible by 3 and $m, m' \in \mathbb{Z}$ (we can do this by the previous paragraph). Thus $v, v' \in \mathcal{O}_K^*$ by (a).

Now suppose 3 ramifies. Since $\mathfrak{P}$ is not principal (if it were principal then 3 or -3 is in K^{*2}, a contradiction) but $\mathfrak{P}^2$ is we get $(\Delta) = \mathfrak{P}^{2k}$ for some $k \in \mathbb{N}$. Thus $\Delta = 3^k u$ for some $u \in \mathcal{O}_K^*$ and (along with 1. and the fact from 2 paragraphs ago) we have $\tau = 3^m v, \tau' = 3^{m'} v'$ where $v, v' \in \mathcal{O}_K^*$ and $m, m' \in \mathbb{Z}$.

Consequently (regardless of whether 3 ramifies),

$$\frac{c_4^3}{3^k u} = \frac{c_4^3}{\Delta} = \frac{(\tau+27)(\tau+3)^3}{\tau} = \frac{(3^m v+27)(3^m v+3)^3}{3^m v},$$

so

$$\frac{c_4^3}{(3^m v+3)^3} = \frac{(3^m v+27)(3^{m-6e+3ord_{(3)}(c_4)} u)}{3^m v},$$

making

$$\frac{(v^{\frac{1}{3}})^3 c_4^3 3^{6e}}{(u^{\frac{1}{3}})^3 (\tau+3)^3 (3^{ord_{(3)}(c_4)})^3} = 3^m v + 27$$

where $u^{\frac{1}{3}}$ (resp. $v^{\frac{1}{3}}$) denotes the unique cube root of u (resp. v) in K and e denotes the ramification index of 3 in K (note that $\tau + 3 \neq 0$ since otherwise $j(E) = 0$ contradicting $\text{ord}_{\mathfrak{P}}(j(E)) < 0$).

Then we have $x \in \mathcal{O}_K$ with $x^3 - 27 = 3^m v$. Thus, $(x-3)(x^2+3x+9) = 3^m v$, so $x - 3 = 3^n w$ for some $w \in \mathcal{O}_K^*$ with $0 \leq n \leq m$. Thus, $x = 3 + 3^n w$, so $x^2 + 3x + 9 = 3^{m-n} v w^{-1}$, yielding $3^{2n} w^2 + 3^{n+2} w + 27 = 3^{m-n} v w^{-1}$. We recall that $m > 4$. If $n = 0$ then $w^2 + 9w + 27$ is coprime

to $\mathfrak{P}$; that is, $3^m vw^{-1}$ is coprime to $\mathfrak{P}$ making $m = 0$, a contradiction. If $n = 1$ then, since $\mathfrak{P}$ is the unique prime of K lying above (3), we see that $\mathrm{ord}_{\mathfrak{P}}(3^{2n}w^2 + 3^{n+2}w + 27)$ is 2 if 3 is inert in K, and is 4 if 3 ramifies in K. This would make $m = 3$ in both cases (inert or ramified). Thus $n \geq 2$ holds. But then $\mathrm{ord}_{\mathfrak{P}}(3^{2n}w^2 + 3^{n+2}w + 27) = 3$ (resp. $= 6$) if 3 is inert (resp. if 3 ramifies). But $3^{2n}w^2 + 3^{n+2}w + 27 = 3^{m-n}vw^{-1}$. Thus, $m - n = 3$ always holds. Then, $x^2 + 3x + 9 = 27w_0$ where $w_0 \in \mathcal{O}_K^*$.

Suppose $K \neq \mathbb{Q}(\sqrt{-1})$. Thus $\mathcal{O}_K^* = \{1, -1\}$, so $v, w \in \{1, -1\}$. This makes $t^3 - 27 + 3^m vw^{-1} \in \mathbb{Z}[t]$. But this cubic polynomial has a root over K. Since $K/\mathbb{Q}$ is quadratic it follows that $t^3 - 27 + 3^m v$ has a root in $\mathbb{Z}$.

Thus we can (and do) assume that $x \in \mathbb{Z}$. Since $x^2 + 3x + 9 - 27w_0 = 0$ and $w_0 \in \mathcal{O}_K^* = \{1, -1\}$, we get $w_0 = 1$, because $w_0 = -1$ gives that $x^2 + 3x + 36 = 0$, a contradiction since $t^2 + 3t + 36 \in \mathbb{Z}[t]$ is irreducible. Thus $x^2 + 3x - 18 = 0$ so $x \in \{3, -6\}$. If $x = 3$ then, as $x^3 - 27 = 3^m v$, we get $m = 0$, a contradiction. Thus $x = -6$ holds and so $m = 3$, since $x^3 - 27 = 3^m v$. This contradicts $m > 4$. Thus, the proof is complete in the case that $K \neq \mathbb{Q}(\sqrt{-1})$

Thus, assume K equals $\mathbb{Q}(\sqrt{-1})$. Now if $w_0 = -1$ the polynomial $t^2 + 3t + 9 - 27w_0$ has discriminant equal to -135. Since $\sqrt{-135} \notin \mathbb{Q}(\sqrt{-1})$ we get that this polynomial is irreducible over K, contradicting that x is a root of it. Similarly, if $w_0 = i$ or $-i$ then the discriminant is $-27 + 108w_0$, which does not have a square root in $\mathbb{Q}(\sqrt{-1})$, because its norm (down to $\mathbb{Q}$) is 12393, which is not itself a square in $\mathbb{Z}$. If $w_0 = 1$ then $x \in \{3, -6\}$ and we get a contradiction on m, just as in the previous paragraph. $\square$

Chapter 5

Non-existence results

We now relate our results to a conjecture of Cremona (see the Introduction in [Cre2]). Let K be a quadratic imaginary number field and $\mathfrak{p}$ a (non-zero) prime ideal of $\mathcal{O}_K$. We have

$$\Gamma_0(\mathfrak{p}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_K) : c \in \mathfrak{p} \right\}.$$

Recall hyperbolic three-space $H_3 := \{(z,t) : z \in \mathbb{C}, t \in \mathbb{R}_{>0}\}$. We then have $H_3^* := H_3 \cup K \cup \{\infty\}$. There is a natural action of $\Gamma_0(\mathfrak{p})$ on H_3^*, allowing us to consider the homology group $H_1(\Gamma_0(\mathfrak{p})\backslash H_3^*, \mathbb{Q})$. There is a natural involution on this space, and we consider the eigenspace associated to the eigenvalue 1, denoted by $V^+(\mathfrak{p})$. We note that this subspace is isomorphic to the space of weight 2 cuspidal automorphic forms for $\Gamma_0(\mathfrak{p})$. Cremona conjectures (see 3.7 in [Cre2]) that there exists an elliptic curve over a quadratic imaginary number field having prime conductor $\mathfrak{p}$ only when there is an element of $V^+(\mathfrak{p})$ that satisfies certain properties (see pg. 278 in [Cre2]).

Applying this to the data in the files for $\mathbb{Q}(\sqrt{-19})$ and $\mathbb{Q}(\sqrt{-67})$ found in [Cre3], it is then conjectured that $p = 19$ is the smallest prime number such that there is an elliptic curve defined over $\mathbb{Q}(\sqrt{-19})$ of prime conductor (π) with $p \in (\pi)$. Corollary 4.10 verifies this claim. For $\mathbb{Q}(\sqrt{-67})$ it is conjectured that 11 is the smallest prime such that there is an elliptic curve of prime conductor (π) with $p \in (\pi)$. Corollary 4.10 verifies this except it cannot rule out the existence of an elliptic curve of prime conductor dividing either 3 or 5.

Remark 5.1. Note that there are exactly 95 primes less than 500.

In the table 4.2 below, we summarize some of what is known. In each column, other than the first and last, we count the number of primes $p \leq 500$ having a certain respective property. In the first column the number fields are listed.

The second column counts the number of p occurring for the given field in Corollary 4.10. The next column gives the number of p having a non-existence result via [Shu] (in [Shu] see Corollary 3.3, Corollary 4.2, Corollary 5.3, Corollary 6.3a, and Corollary 7.2).

In the next column we have the number of p for which there is an elliptic curve, over $\mathbb{Q}$, of conductor p where p is inert in K. These curves can be found in the tables of [Cre1]. Any such curve gives an elliptic curve, over K, of prime conductor. The fifth column gives the primes p, for which, there is an elliptic curve, over K, of prime ideal conductor $\mathfrak{p}$, where $p \in \mathfrak{p}$. There curves are those found in tables 3.2.3, 3.3.3, 3.4.3, 3.5.3, and 3.6.3 of [Cre2] and the tables in [Cre4]. The next column lists the totals for each row. A given K may have primes contributing to both column 2 and column 3 (resp. contributing to both column 4 and column 5). Each total, though, counts a prime only once.

Finally, the next to last column gives the percentage of primes $p \leq 500$ for which we know, with proof, whether there exists an elliptic curve, over K, of prime conductor $\mathfrak{p}$ with $p \in \mathfrak{p}$. The last column gives, for each K, the smallest prime not included in the total from the previous column.

K	4.10	[Shu] lists	[Cre1] table	[Cre4] lists	total	%	first prime
$\mathbb{Q}(\sqrt{-1})$	50	61	18	4	87	91.57	23
$\mathbb{Q}(\sqrt{-2})$	0	58	13	0	71	74.73	3
$\mathbb{Q}(\sqrt{-3})$	0	28	19	4	51	53.68	23
$\mathbb{Q}(\sqrt{-7})$	53	26	13	0	73	76.84	13
$\mathbb{Q}(\sqrt{-11})$	0	41	18	3	62	65.26	2
$\mathbb{Q}(\sqrt{-19})$	45	0	14	1	60	63.15	31
$\mathbb{Q}(\sqrt{-43})$	45	0	17	1	63	66.31	2
$\mathbb{Q}(\sqrt{-67})$	42	0	18	1	61	64.21	3
$\mathbb{Q}(\sqrt{-163})$	32	0	21	0	53	55.78	5

Table 5.2

Chapter 6

a review of arithmetical graphs

An arithmetical graph consists of three objects (as introduced and developed in [Lor1]). The first is a connected graph G with V_G, the set of vertices of G, having exactly $2 \leq n$ elements. We allow for there to be multiple edges between distinct vertices of the graph but do not allow any self-loops. In addition we require each vertex to have a positive integer multiplicity attached to it. We always want to fix an ordering on the vertices $v_1, v_2, ..., v_n$. Then to each v_i we associate a positive integer multiplicity r_i. We require this to be done in such a manner that for each v_i we have $r_i | \sum r_j$, where the sum is taken over all vertices adjacent to v_i. We then get the vector $R = (r_1, r_2, ..., r_n)^t \in \mathbb{Z}^n$. We then form a symmetric $(n \times n)$-matrix M where for $i \neq j$ we have $M_{i,j} := -$(the number of edges between v_i and v_j) and for the diagonal entries we uniquely put in positive integers so that $M \cdot R$ is the zero vector in $\mathbb{Z}^n$. An *arithmetical graph* is then the triple (G, M, R).

We will call an element $D \in \mathbb{Z}^n$ a *divisor*. The matrix R^t defines the $\mathbb{Z}$-module homomorphism R^t: $\mathbb{Z}^n \to \mathbb{Z}$ by $D \mapsto R^t \cdot D$. The matrix M defines a $\mathbb{Z}$-module homomorphism M: $\mathbb{Z}^n \to \mathbb{Z}^n$ by $D \mapsto M \cdot D$. The *degree* of D is then defined as the integer $R^t \cdot D$. By symmetry of M and $M \cdot R$ being zero we see that $R^t \cdot M$ is zero making $R^t \cdot (M \cdot D)$ zero; that is, $\mathrm{im}(M) \subset \ker(R^t)$ and we form the quotient group $\ker(R^t)/\mathrm{im}(M)$. This is a finite Abelian group. We denote it by $\Phi(M)$ and its order by $\phi(M)$.

We will call such a D *effective* if each component of D is non-negative. Two divisors D_1, D_2 will be called *equivalent* if $D_1 - D_2 \in \mathrm{im}(M)$. We put $[D] := \{D^{'} \in \mathbb{Z}^n : D \text{ is equivalent to } D^{'}\}$. We define the *g-integer*, denoted $g(M)$, as the smallest non-negative integer such that every divisor of degree at least $g(M)$ is equivalent to an effective divisor (see Proposition 1.6 [Lor2] for the existence of such an integer). Related to this is the invariant $\rho(M)$, defined to be the smallest non-negative integer such that there is an effective divisor of degree d whenever $\rho(M) \leq d$. It is clear that $\rho(M) \neq 1$ and also that $\rho(M) \leq g(M)$.

Let d_i denote the number of edges incident to v_i. We let $\beta(M)$ denote the Betti number of G, so $2 \cdot \beta(M) - 2 := \sum_{i=1}^{n} (d_i - 2)$. A natural way to extend this concept is to include the

multiplicities of the vertices in the sum. We thus define the *linear rank*, denoted $g_0(M)$, by

$$2 \cdot g_0(M) - 2 = \sum_{i=1}^{n} r_i(d_i - 2).$$

Also, we have

$$\mathfrak{C}(M) := \{[K] : \deg(K) = 2g(M) - 2 \text{ and } K - E \text{ is equivalent to an effective divisor whenever } E \text{ is an effective divisor of degree } g(M) - 1\}.$$

We will say that K is a *canonical divisor* for M if $[K] \in \mathfrak{C}(M)$.

An arithmetical graph is called *minimal* if $2 \leq M_{i,i}$ for all $i \in \{1, ...n\}$ and is called an *arithmetical tree* when G is a *tree* (i.e., $\beta(M) = 0$). A vertex v_i is called a *node* if $d_i \geq 3$. It is called *terminal* if $d_i = 1$. A *connecting chain* (resp. *terminal chain*) is a path in G between two nodes (resp. between a node and a terminal vertex). The *weight* of a chain is defined to be $\gcd\{r_i : v_i \text{ is in the chain}\}$. Finally, a node is called a *terminal node* it has exactly one connecting chain attached to it.

We can look to arithmetic geometry as a source of arithmetical graphs. Let F be a discrete valuation field. By a *curve* over F, X/F, we mean a 1-dimensional F-scheme that is smooth, proper, geometrically irreducible whose genus, $p_g(X)$, is positive. In particular we see that a curve is projective. By a *regular model* for a curve X/F we mean a connected regular $\mathcal{O}_F$-scheme that is proper and is such that its generic fiber is isomorphic over F to X/F. Every curve over F has a regular model.

For a curve X/F and a model $\mathfrak{X}/\mathcal{O}_F$ we can consider the k-scheme $\mathfrak{X}_k$, the special fiber. We know that the number of irreducible components of $\mathfrak{X}_k$ is finite. Denote these as $C_1, ..., C_n$ and let the positive integers $r_1, ..., r_n$ denote their respective multiplicities. Attached to this model we have the so-called intersection matrix, which is defined to be the $(n \times n)$-matrix M where

$$M_{ij} := -(C_i \cdot C_j).$$

Note that $M \cdot R$ is zero where $R := (r_1, ..., r_n)^t$. We will let G be the connected graph whose vertices correspond to the irreducible components and whose edges, between distinct vertices v_i and v_j, are equal in number to $(C_i \cdot C_j)$.

Note that if $X(K) \neq \emptyset$ then $\gcd(r_1, ..., r_n) = 1$. Note that if we choose another regular model of X/K, say one with $s_1, ..., s_m$ as the associated sequence of multiplicities, then

$$\gcd(r_1, ..., r_n) = \gcd(s_1, ...s_m).$$

Unless otherwise stated, we will assume, for a curve in question, that this gcd equals 1. In light of this assumption, it is shown in [Ray] that when k is algebraically closed we have that $\ker(R^t)/\mathrm{im}(M)$ is isomorphic to the group of k-rational points of the scheme of components of the special fiber of the Néron model of $\mathrm{Jac}(X)/F$.

Conversely, every arithmetical graph (G, M, R) occurs as the degeneration of a curve as above (see [Win]).

Chapter 7

Gluing two arithmetical graphs and the effect on the g-integer

Take two arithmetical graphs (G, M, R) and $(G^{'}, M^{'}, R^{'})$. Let n and m denote respectively the number of vertices of G and $G^{'}$. Take the unique pair of positive integers $(h, h^{'})$ where $\gcd(h, h^{'}) = 1$ and simultaneously $h \cdot r_n = h^{'} \cdot r_1^{'}$. One easily checks that $\gcd(r_n, r_1^{'}) = \frac{r_n \cdot r_1^{'}}{r}$. Put $r := h \cdot r_n = h^{'} \cdot r_1^{'}$. We get from these two arithmetical graphs another arithmetical graph by in effect gluing G (at its vertex v_n) to $G^{'}$ (at its vertex $v_1^{'}$).

Definition 7.1. The *join* of (G, v_n) to $(G^{'}, v_1^{'})$ is an arithmetical graph $(G^{''}, M^{''}, R^{''})$ on $n + m - 1$ vertices where for $1 \leq i, j \leq n + m - 1$

$$M_{i,j}^{''} := \begin{cases} M_{i,j} & \text{if } i, j \leq n \text{ and } (i, j) \neq (n, n) \\ M_{i-n+1, j-n+1}^{'} & \text{if } n \leq i, j \text{ and } (i, j) \neq (n, n) \\ M_{n,n} + M_{1,1}^{'} & \text{if } (i, j) = (n, n) \\ 0 & \text{else} \end{cases}$$

and

$$R^{''t} := (h \cdot r_1, h \cdot r_2, ..., h \cdot r_{n-1}, r, h^{'} \cdot r_2^{'}, ..., h^{'} \cdot r_m^{'}).$$

When it is clear from the context what the two vertices are where the join is performed we will simply call it the join of G to $G^{'}$ and write it as $G \oplus G^{'}$, in which case we may denote $M^{''}$ by $M \oplus M^{'}$.

Definition 7.2. The arithmetical graphs that can be constructed as a join where $(h, h^{'}) = (1, 1)$ will be called *reducible*. All other arithmetical graphs will be called *irreducible*. For the purpose of distinction we may use the phrase *simple join* when we are in the case that $(h, h^{'}) = (1, 1)$.

Finally, it is clear that the operation of join is commutative, in the sense that $(G \oplus G^{'}, M \oplus M^{'}, R^{''})$ is explicitly isomorphic to the arithmetical graph that is associated to $M^{'} \oplus M$.

7.3. One easily checks that $g_0(M^{''}) = h \cdot (g_0(M) - 1) + h^{'} \cdot (g_0(M^{'}) - 1) + r + 1$.

It turns out, however, that the g-integer does not transform in the exact same way. The following result, nonetheless, gives a lower bound.

Proposition 7.4. *Let* (G'', M'', R'') *be the join of* (G, M, R) *and* (G', M', R'). *We have* $g(M'') = h \cdot (g(M) - 1) + h' \cdot (g(M') - 1) + r + 1 + \epsilon$ *where* $0 \leq \epsilon \leq M''_{n,n} \cdot r \cdot (r-1)$.

Proof : First we show that $h \cdot (g(M)-1)+h' \cdot (g(M')-1)+r+1 \leq g(M'')$. Take $\begin{pmatrix} A \\ a \end{pmatrix} \in$ $\mathrm{Div}(M)$ of degree $g(M) - 1$ that is not equivalent to an effective divisor. Also, take $\begin{pmatrix} b \\ B \end{pmatrix} \in$ $\mathrm{Div}(M')$ of degree $g(M') - 1$ that is not equivalent to an effective divisor. Now $\begin{pmatrix} A \\ a+b+1 \\ B \end{pmatrix}$ $\in \mathrm{Div}(M'')$ has degree $h \cdot (g(M)-1)+h' \cdot (g(M')-1)+r$. Suppose $\begin{pmatrix} A \\ a+b+1 \\ B \end{pmatrix}$ is equivalent to some effective divisor. Thus,

$$\begin{pmatrix} A \\ a+b+1 \\ B \end{pmatrix} = M'' \cdot D + E = (x_1, ..., x_{n-1}, x_n + y_1, y_2, ..., y_m)^t + E.$$

where

$$E := (e_1, ..., e_{n+m-1})^t \text{ is effective, } (x_1, ..., x_n)^t \in \mathrm{im}(M), \text{ and } (y_1, ..., y_m)^t \in \mathrm{im}(M').$$

But then

$$\begin{pmatrix} A \\ a \end{pmatrix} = (x_1, ...x_n)^t + (0, 0, ..., 0, y_1 - b - 1)^t + (e_1, ...e_n)^t.$$

and

$$\begin{pmatrix} b \\ B \end{pmatrix} = (y_1, ...y_m)^t + (x_n - a - 1, 0, 0, ..., 0)^t + (e_n, e_{n+1}, ..., e_{n+m-1})^t.$$

By $\begin{pmatrix} A \\ a \end{pmatrix}$ and $\begin{pmatrix} b \\ B \end{pmatrix}$ each individually not being equivalent to an effective divisor we find that $y_1 - b - 1 + e_n < 0$ and $x_n - a - 1 + e_n < 0$; that is, $y_1 + e_n < b+1$ and $x_n + e_n < a+1$. But

$x_n+y_1+e_n = a+b+1$ (so $x_n+y_1+e_n+1 = a+b+2$) making $y_1+x_n+2e_n < x_n+y_n+e_n+1$, which implies that $e_n < 1$. As $0 \leq e_n$ we get $e_n = 0$. Thus, $y_1 < b+1$ and $x_n < a+1$; that is, $y_1 \leq b$ and $x_n \leq a$. But from $x_n + y_1 = a + b + 1$ we then get $a + b + 1 \leq a + b$, a contradiction. Consequently, $\begin{pmatrix} A \\ a+b+1 \\ B \end{pmatrix}$ is not equivalent to an effective divisor, so we must have $h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1 \leq g(M^{''})$.

Now suppose that $g(M^{''}) > h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1 + M^{''}_{n,n} \cdot r^2$. Thus there is a divisor in $\mathrm{Div}(M^{''})$ of degree $h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1 + M^{''}_{r,r} \cdot r^2 + c$ (with $0 \leq c$) that is not equivalent to an effective. As $G^{''}$ has a vertex of multiplicity r we can and do assume that $c < r$. But this fact also tells us that we can subtract off the divisor $\begin{pmatrix} 0 \\ M^{''}_{n,n} \cdot r \\ 0 \end{pmatrix}$ and end up with a divisor that is also not equivalent to an effective. Thus we have $\begin{pmatrix} A \\ \alpha \\ B \end{pmatrix} \in \mathrm{div}(M^{''})$ of degree $h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1 + c$ such that

$$\begin{pmatrix} A \\ \alpha \\ B \end{pmatrix} + \begin{pmatrix} 0 \\ M^{''}_{n,n} \cdot r \\ 0 \end{pmatrix}$$

is not equivalent to an effective.

There is $\ell \in \mathbb{Z}$ such that

$$h \cdot (g(M) - 1) + 1 \leq \deg_{M''} \begin{pmatrix} A \\ \alpha + \ell \end{pmatrix} \leq h \cdot (g(M) - 1) + r$$

and

$$h^{'} \cdot (g(M^{'}) - 1) + 1 \leq \deg_{M''} \begin{pmatrix} -\ell \\ B \end{pmatrix}.$$

To see this is possible note that the effect on the degree that happens when we add $\begin{pmatrix} 0 \\ \ell \end{pmatrix}$ onto $\begin{pmatrix} A \\ \alpha \end{pmatrix}$ is adding $r \cdot \ell$. This then gives

$$\frac{h\cdot(g(M)-1)+1}{h} \leq \deg_M \begin{pmatrix} A \\ \alpha+\ell \end{pmatrix}$$

and

$$\frac{h^{'}\cdot(g(M^{'})-1)+1}{h^{'}} \leq \deg_{M'} \begin{pmatrix} -\ell \\ B \end{pmatrix}$$

These then give respectively that

$$g(M) \leq \deg_M \begin{pmatrix} A \\ \alpha+\ell \end{pmatrix}$$

and

$$g(M^{'}) \leq \deg_{M'} \begin{pmatrix} -\ell \\ B \end{pmatrix}$$

Thus

$$\begin{pmatrix} A \\ \alpha+\ell \end{pmatrix} = M \cdot D_1 + E$$

and

$$\begin{pmatrix} -\ell \\ B \end{pmatrix} = M^{'} \cdot D_1^{'} + E^{'}$$

where

$$E := (e_1, ..., e_n)^t \text{ and } E^{'} := (e_1^{'}, ..., e_m^{'})^t \text{ are both effective.}$$

But then $\begin{pmatrix} A \\ \alpha \\ B \end{pmatrix} + \begin{pmatrix} 0 \\ M_{n,n}^{''} \cdot r \\ 0 \end{pmatrix} =$

$$M^{''} \cdot \begin{pmatrix} d_{1_1} \\ \vdots \\ d_{1_{n-1}} \\ d_{1_n} + d_{1_1}^{'} \\ d_{1_2}^{'} \\ \vdots \\ d_{1_m}^{'} \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ d_{1_1}^{'} \\ \vdots \\ d_{1_1}^{'} \\ -d_{1_1}^{'} M_{n,n} - d_{1_n} M_{1,1}^{'} \\ d_{1_n} \\ \vdots \\ d_{1_n} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_{n-1} \\ e_n + e_1^{'} \\ e_2^{'} \\ \vdots \\ e_m^{'} \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ M_{n,n}^{''} \cdot r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Now we can and do assume that both D_1 and $D_1^{'}$ are such that $0 \leq d_{1_n}, d_{1_1}^{'} \leq r-1$. This makes $-M_{n,n}^{''} \cdot (r-1) \leq -d_{1_1}^{'} M_{n,n} - d_{1_n} M_{1,1}^{'}$, yielding that $\begin{pmatrix} A \\ \alpha \\ B \end{pmatrix} + \begin{pmatrix} 0 \\ M_{n,n}^{''} \cdot (r-1) \\ 0 \end{pmatrix}$ is equivalent to an effective, a contradiction. □

The ϵ in Proposition 7.4 has another upper bound. By the fact $g(M) \leq g_0(M^{''})$, we immediately get by combining 7.3 and Proposition 7.4 that

$$h \cdot (g_0(M) - 1) + h^{'} \cdot (g_0(M^{'}) - 1) + r + 1 = h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1 + \epsilon.$$

Consequently, we get the bound

Remark 7.5. $\epsilon \leq h \cdot (g_0(M) - g(M)) + h^{'} \cdot (g_0(M^{'}) - g(M^{'}))$.

Corollary 7.6. *Let $(G^{''}, M^{''}, R^{''})$ be the join of (G, M, R) and $(G^{'}, M^{'}, R^{'})$. If $g(M) = g_0(M)$ and $g(M^{'}) = g_0(M^{'})$ then $g(M^{''}) = g_0(M^{''})$.*

Proof : By Remark 7.5 we know that the ϵ in Proposition 7.4 must equal 0. Thus,

$$g(M^{''}) = h \cdot (g(M) - 1) + h^{'} \cdot (g(M^{'}) - 1) + r + 1.$$

Since $g(M^{'}) = g_0(M^{'})$ and $g(M^{''}) = g_0(M^{''})$ by hypothesis we get

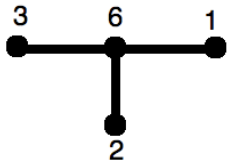
$$g(M^{''}) = h \cdot (g_0(M) - 1) + h^{'} \cdot (g_0(M^{'}) - 1) + r + 1.$$

By 7.3 this says $g(M^{''}) = g_0(M^{''})$. □

Corollary 7.7. *Let $(G^{''}, M^{''}, R^{''})$ be the join of (G, M, R) and $(G^{'}, M^{'}, R^{'})$. If $r = 1$ then $g(M^{''}) = g(M) + g(M^{'}) + r - 1$.*

Proof : Since $r = 1$ we get $h = h^{'} = 1$. The result is then immediate from Proposition 7.4 □

Example 7.8. It is however possible for the ϵ in Proposition 7.4 to be strictly positive. For an example take



This graph has g-integer 0. If we join this graph to itself at the node then the resulting graph has g-integer 7 (see Appendix C for the computation), making $\epsilon = 2$ in the formula for Proposition 7.4. □

Proposition 7.9. *Let (G, M, R) and $(G^{'}, M^{'}, R^{'})$ be two arithmetical graphs. We have $\phi(M \oplus M^{'}) = \phi(M) \cdot \phi(M^{'}) \cdot \ gcd(r_n, r_1^{'})^2$.*

Proof : By Corollary 1.3 and Theorem 1.4 in [Lor1] we have

$$\phi(M \oplus M^{'}) = \frac{det(M \oplus {M^{'}}^{n,n})}{r \cdot r},$$

$$\phi(M) = \frac{det(M^{n,n})}{r_n \cdot r_n},$$

and

$$\phi(M^{'}) = \frac{det({M^{'}}^{1,1})}{r_1^{'} \cdot r_1^{'}}.$$

By the way in which $M \oplus M^{'}$ is formed from M and $M^{'}$ we see that

$$\det(M \oplus {M^{'}}^{n,n}) = \det(M^{n,n}) \cdot \det({M^{'}}^{1,1}).$$

Thus, $\phi(M \oplus M^{'}) \cdot r^2 = \phi(M) \cdot r_n^2 \cdot \phi(M^{'}) \cdot {r_1^{'}}^2$ making

$$\phi(M \oplus M^{'}) = \phi(M) \cdot \phi(M^{'}) \cdot (\frac{r_n \cdot r_1^{'}}{r})^2 = \phi(M) \cdot \phi(M^{'}) \cdot \gcd(r_n, r_1^{'})^2,$$

as claimed. □

Chapter 8

The g-integer and Blow-ups

In this chapter we examine how certain invariants change under a blow-up. We start by recalling the definition of a blow-up (see 1.8 in [Lor1] for additional facts). Take an effective divisor $Q := (q_1, ..., q_n)^t \in \mathbb{Z}^n$ and form the $(n+1 \times n+1)$-matrix

$$M_Q := \begin{pmatrix} M + Q \cdot Q^t & -Q \\ -Q^t & 1 \end{pmatrix}$$

Assume for the rest of this chapter that M_Q is the intersection matrix associated to an arithmetical graph (G_Q, M_Q, R_Q) where $R_Q = (r_1, ..., r_n, \sum q_i r_i)^t$.

We first note that for $B \in \mathrm{Div}(M)$ and $b \in \mathbb{Z}$ we have

$$M_Q \cdot \begin{pmatrix} B \\ b \end{pmatrix} = \begin{pmatrix} M + Q \cdot Q^t & -Q \\ -Q^t & 1 \end{pmatrix} \cdot (b_1, ..., b_n, b)^t.$$

$$= \begin{pmatrix} M \cdot B \\ 0 \end{pmatrix} + \Big(q_1(-b + \sum q_i b_i), q_2(-b + \sum q_i b_i), ..., q_n(-b + \sum q_i b_i), b - \sum q_i b_i\Big)^t \ (*)$$

and hence

$$\begin{pmatrix} M \cdot B \\ 0 \end{pmatrix} = M_Q \cdot \begin{pmatrix} B \\ b \end{pmatrix} + \Big(q_1(b - \sum q_i b_i), q_2(b - \sum q_i b_i), ..., q_n(b - \sum q_i b_i), -b + \sum q_i b_i\Big)^t \ (**).$$

Proposition 8.1. *Keep the notation as above. Then have $g(M_Q) = g(M)$.*

Proof : First we show $g(M) \leq g(M_Q)$. Suppose $g(M_Q) < g(M)$. Take $D \in \mathrm{Div}(M)$ of degree $g(M) - 1$ that is not equivalent to some effective divisor. Thus, as $g(M_Q) \leq g(M) - 1$ we have for $\begin{pmatrix} D \\ 0 \end{pmatrix} \in \mathrm{Div}(M_Q)$ that $\begin{pmatrix} D \\ 0 \end{pmatrix} = M_Q \cdot D' + E$ for some $D', E \in \mathrm{Div}(M_Q)$ where $E \geq 0$. Thus, by (**) we get

$$D = M \cdot (d_1', ..., d_n')^t + (e_1, ..., e_n)^t + \Big(q_1(-d_{n+1}' + \sum q_i d_i'), ..., q_n(-d_{n+1}' + \sum q_i d_i')\Big)^t.$$

and we also get

$$0 = d_{n+1}^{'} + e_{n+1} - \sum q_i d_i^{'}.$$

If we show that each entry of this last column vector is non-negative then clearly we will have reached a contradiction. Now each entry is non-negative if (since each $q_i \geq 0$) $\sum q_i d_i^{'} \geq d_{n+1}^{'}$. But $-e_{n+1} = d_{n+1}^{'} - \sum q_i d_i^{'}$ and $0 \leq e_{n+1}$, so indeed $\sum q_i d_i^{'} \geq d_{n+1}^{'}$. Consequently, we conclude that $g(M) \leq g(M_Q)$.

Now we will show that $g(M_Q) \leq g(M)$. Suppose $g(M) < g(M_Q)$. Take $\begin{pmatrix} D \\ \alpha \end{pmatrix} \in \text{Div}(M_Q)$ having degree $g(M_Q) - 1$ that is not equivalent to some effective divisor. Thus $D + \alpha Q \in \text{Div}(M)$ has degree $g(M_Q) - 1$ since

$$(r_1, ..., r_n, \sum r_i q_i)^t.$$

is the kernel vector for M_Q. Now since $g(M) \leq g(M_Q) - 1$ we get

$$D + \alpha Q = M \cdot D^{'} + E$$

for some $D^{'}, E \in \text{Div}(M)$ where $E \geq 0$. Thus

$$\begin{pmatrix} D + \alpha Q \\ 0 \end{pmatrix} = \begin{pmatrix} M \cdot D^{'} \\ 0 \end{pmatrix} + \begin{pmatrix} E \\ 0 \end{pmatrix}$$

making

$$\begin{pmatrix} D \\ \alpha \end{pmatrix} = \begin{pmatrix} M \cdot D^{'} \\ 0 \end{pmatrix} + \begin{pmatrix} E \\ 0 \end{pmatrix} - \begin{pmatrix} \alpha Q \\ -\alpha \end{pmatrix}$$

$$= \begin{pmatrix} M \cdot D^{'} \\ 0 \end{pmatrix} + \begin{pmatrix} E - \alpha Q \\ \alpha \end{pmatrix}.$$

This along with

$$M_Q \cdot \begin{pmatrix} D^{'} \\ \delta \end{pmatrix} = \begin{pmatrix} M \cdot D^{'} \\ 0 \end{pmatrix} + \Big(q_1(-\delta + \sum q_i d_i^{'}), q_2(-\delta + \sum q_i d_i^{'}), ..., q_n(-\delta + \sum q_i d_i^{'}), \delta - \sum q_i d_i^{'} \Big)^t$$

gives

$$\begin{pmatrix} D \\ \alpha \end{pmatrix} =$$

$$M_Q \cdot \begin{pmatrix} D^{'} \\ \delta \end{pmatrix} - \Big(q_1(-\delta + \sum q_i d_i^{'}), ..., q_n(-\delta + \sum q_i d_i^{'}), 0 \Big)^t - (0, 0, ..., 0, \delta - \sum q_i d_i^{'})^t + \begin{pmatrix} E - \alpha Q \\ \alpha \end{pmatrix}$$

$$=M_Q \cdot \begin{pmatrix} D' \\ \delta \end{pmatrix} + \Big(e_1 - q_1(\alpha - \delta + \sum q_i d_i'), ..., e_n - q_n(\alpha - \delta + \sum q_i d_i'), \alpha - \delta + \sum q_i d_i'\Big)^t.$$

Thus, if $\delta := \alpha + \sum q_i d_i'$ then for each $1 \leq i \leq n$ the i^{th} entry in this last column vector equals e_i while the last entry equals 0. Thus we have a contradiction and consequently the proposition is proven. □

Remark 8.2. Since $g_0(M) \leq g_0(M_Q)$ (see Lemma 2.10 in [Lor3]) we get by Proposition 8.1 that $g_0(M) - g(M) \leq g_0(M_Q) - g(M_Q)$.

We have the following fact for blow-ups. Recall that we have the explicit group isomorphism

$$\Theta : \mathbb{Z}^n/\mathrm{im}(M) \to \mathbb{Z}^{n+1}/\mathrm{im}(M_Q).$$

defined by $[D] \longmapsto [\begin{pmatrix} D \\ 0 \end{pmatrix}]$. We know Θ is well-defined and injective since

$$D_1 - D_2 \in \mathrm{im}(M) \text{ if and only if } \begin{pmatrix} D_1 \\ 0 \end{pmatrix} - \begin{pmatrix} D_2 \\ 0 \end{pmatrix} \in \mathrm{im}(M_Q).$$

It is surjective since

$$(q_1, q_2, ..., q_n, -1) \in \mathrm{Im}(M_Q).$$

Since Θ preserves degree we find that restricting Θ to the subgroup $\Phi(M)$ yields

$$\Phi(M) \cong \Phi(M_Q).$$

Proposition 8.3. *We have $\mathfrak{C}(M) \neq \emptyset$ if and only if $\mathfrak{C}(M_Q) \neq \emptyset$ (see Chapter 5 for the notation). In fact we know that if K is a canonical divisor for M then $\begin{pmatrix} K \\ 0 \end{pmatrix}$ is a canonical divisor for M_Q and that if $\begin{pmatrix} K \\ k \end{pmatrix}$ is a canonical divisor for M_Q then $K + (k \cdot q_1, ..., k \cdot q_n)^t$ is a canonical divisor for M. Moreover, restricting $\Theta|_{\mathfrak{C}(M)}$ yields a set bijection*

$$\mathfrak{C}(M) \cong \mathfrak{C}(M_Q).$$

Proof : Suppose K is a canonical divisor for M and suppose $\begin{pmatrix} E \\ e \end{pmatrix} \in \mathrm{Div}(M_Q)$ is an effective divisor of degree $g(M_Q) - 1$. Thus $E + (e \cdot q_1, ..., e \cdot q_n)^t \in \mathrm{Div}(M)$ is an effective divisor of degree $g(M_Q) - 1$. Thus by Proposition 8.1 this divisor has degree $g(M) - 1$. Consequently,

$$K - E - (e \cdot q_1, ..., e \cdot q_n)^t = M \cdot B + E'$$

for some $B, E' \in \mathrm{Div}(M)$ where E' is effective. This makes

$$\begin{pmatrix} K \\ 0 \end{pmatrix} - \begin{pmatrix} E \\ e \end{pmatrix} = \begin{pmatrix} M \cdot B \\ 0 \end{pmatrix} + \begin{pmatrix} E' \\ 0 \end{pmatrix} + (e \cdot q_1, ..., e \cdot q_n, -e)^t$$

in turn making $\begin{pmatrix} K \\ 0 \end{pmatrix} - \begin{pmatrix} E \\ e \end{pmatrix} =$

$$M_Q \cdot \begin{pmatrix} B \\ -e + \sum q_i b_i \end{pmatrix} + \begin{pmatrix} q_1(-e + \sum q_i b_i - \sum q_i b_i) \\ q_2(-e + \sum q_i b_i - \sum q_i b_i) \\ . \\ . \\ . \\ q_n(-e + \sum q_i b_i - \sum q_i b_i) \\ -b + \sum q_i b_i \end{pmatrix} + \begin{pmatrix} E' \\ 0 \end{pmatrix} + \begin{pmatrix} eq_1 \\ . \\ . \\ . \\ eq_n \\ -e \end{pmatrix}$$

$$= M_Q \cdot \begin{pmatrix} B \\ -e + \sum q_i b_i \end{pmatrix} + \begin{pmatrix} E' \\ 0 \end{pmatrix}.$$

Thus $\begin{pmatrix} K \\ 0 \end{pmatrix}$ is indeed a canonical divisor for M_Q.

Now we suppose that $\begin{pmatrix} K \\ k \end{pmatrix}$ is a canonical divisor for M_Q and suppose $E \in \mathrm{Div}(M)$ is an effective divisor of degree $g(M) - 1$. Since $g(M_Q) = g(M)$ by Proposition 8.1 we find that $\begin{pmatrix} E \\ 0 \end{pmatrix} \in \mathrm{Div}(M_Q)$ is an effective divisor of degree $g(M_Q) - 1$. Then

$$\begin{pmatrix} K \\ 0 \end{pmatrix} - \begin{pmatrix} E \\ e \end{pmatrix} = M_Q \cdot \begin{pmatrix} B \\ b \end{pmatrix} + \begin{pmatrix} E' \\ e' \end{pmatrix}$$

for some $\begin{pmatrix} B \\ b \end{pmatrix}, \begin{pmatrix} E^{'} \\ e^{'} \end{pmatrix} \in \mathrm{Div}(M_Q)$ where $\begin{pmatrix} E^{'} \\ e^{'} \end{pmatrix} \geq 0$. Thus,

$$\begin{pmatrix} K \\ 0 \end{pmatrix} + (k \cdot q_1, ..., k \cdot q_n, 0)^t - \begin{pmatrix} E \\ 0 \end{pmatrix} = M_Q \cdot \begin{pmatrix} B \\ b \end{pmatrix} + \begin{pmatrix} E^{'} \\ e^{'} \end{pmatrix} + (k \cdot q_1, ..., k \cdot q_n, -k)^t$$

By (*) we then have

$$K + (k \cdot q_1, ..., k \cdot q_n)^t - E = M \cdot B + E^{'} + (q_1(-b + \sum q_i b_i), ..., q_n(-b + \sum q_n b_n))^t + (k \cdot q_1, ..., k \cdot q_n)^t$$

and

$$0 = b - \sum q_i b_i + e^{'} - k.$$

This latter fact says that $0 \leq k - b + \sum q_i b_i$, which shows (as $0 \leq q_i$) that the sum of the last two column vectors is an effective divisor. Therefore, $K + (k \cdot q_1, ..., k \cdot q_n)^t$ is an effective divisor for M. □

We now show how the irreducibility/reducibility nature of an arithmetical graph is often invariant under a blow-up.

Proposition 8.4. *If G is irreducible then G_Q is also irreducible unless Q takes the following shape with respect to some elementary basis vector $E_i = (0, ..., 0, 1, 0, ..., 0)^t$ of $\mathbb{Z}^n$:*

$$Q = q \cdot E_i \text{ for some positive integer } q \text{ and } i \in \{1, .., n\} \text{ for which } r_i = 1.$$

When Q in is this special shape then G_Q is reducible in exactly one way.

Proof : Suppose the blow-up is reducible, say at vertex v_t with $V_1 \cup V_2 = V_{G_Q} - \{v_t\}$ being the associated non-trivial partition of the others vertices in V_{G_Q}. Consequently, we have

$$r_t \mid \sum_{j \in J_1} M_{Q_{t,j}} r_j \text{ and } r_t \mid \sum_{j \in J_2} M_{Q_{t,j}} r_j$$

where for $i \in \{1, 2\}$ we put $J_i := \{j : M_{Q_{t,j}} \neq 0\} \cap V_i$. As $J_1, J_2 \neq \emptyset$ we know these 2 above sums are each non-zero. In light of all this we see that $v_t \neq v_{n+1}$ because

$$-r_{n+1} = -\sum_{i=1}^{n} r_i q_i = \sum_{i=1}^{n} M_{Q_{n+1,i}} r_i.$$

Thus we may and do assume that $v_{n+1} \in V_2$. Hence, $\{V_1, V_2 - \{v_{n+1}\}\}$ gives a partition of $V_G - \{v_t\}$. Moreover, since no vertex in V_1 is connected to some vertex in V_2 in the graph G_Q we know that no vertex in V_1 is connected to some vertex in $V_2 - \{v_{n+1}\}$ in the graph G. In addition we know that the partition splits G, unless it is trivial. Thus we will be able to make G reducible at v_t with this partition provided the partition is non-trivial, $\gcd\{r_i : v_i \in V_1\} = 1$, $\gcd\{r_i : v_i \in V_2 - \{v_{n+1}\}\} = 1$, and $r_t \mid \sum_{j \in J} M_{t,j} r_j$ where $J := \{j : M_{t,j} \neq 0\} \cap V_1$.

Now our partition will be non-trivial unless $V_2 = \{v_{n+1}\}$. If indeed $V_2 = \{v_{n+1}\}$ we use the fact that for $i \neq t$ we have $q_i \neq 0$ only when $v_i \in V_2$ to conclude that $Q = q \cdot E_t$ for some positive integer q. But then we must also have $r_{n+1} = q \cdot r_t$ and moreover there is an arithmetical graph having exactly 2 vertices, one with multiplicity r_t and the other with multiplicity $q \cdot r_t$. Thus, $\gcd(r_t, q \cdot r_t) = 1$, so $r_t = 1$. Then v_t has multiplicity 1 in G. Finally, it is clear by G being irreducible and by the structure of singular and trivial blow-ups that this was in fact the only way to make G_Q reducible.

For the rest of the proof we will assume that $V_2 \neq \{v_{n+1}\}$ and hence our partition is non-trivial. By the way blow-ups are constructed and the fact that no vertex in V_1 is connected, in G_Q, to v_{n+1} we see that $M_{t,j} = M_{Q_{t,j}}$ for all $j \in V_1$, making $J = J_1$. This gives that

$$r_t \mid \sum_{j \in J} M_{t,j} r_j.$$

Since $\{V_1, V_2\}$ is the partition for the way in which we have made G_Q reducible we know that $1 = \gcd\{r_i : v_i \in V_1\}$ and that $1 = \gcd\{r_i : v_i \in V_2\}$. Now as $r_{n+1} = \sum_{i=1}^{n} r_i q_i$ and $v_i \in V_2$ if $q_i \neq 0$ we know that

$$\gcd\{r_i : v_i \in V_2 - \{v_{n+1}\}\} = \gcd\{r_i : v_i \in V_2\} = 1.$$

We are now finished with the proof. □

Proposition 8.5. *If G_Q is irreducible then G is also irreducible.*

Proof : Suppose G is reducible, say at vertex v_t with $V_1 \cup V_2 = V_G - \{v_t\}$ being the associated non-trivial partition of the others vertices in V_G. Now if v_{ℓ_1} and v_{ℓ_2} are distinct vertices in $V_G - \{v_t\}$ that both become connected to v_{n+1} in G_Q then, by the structure of blow-ups, we know that v_{ℓ_1} and v_{ℓ_2} are connected in G. Thus we would have v_{ℓ_1} and v_{ℓ_2} in the same V_i. Thus we may and do assume that v_{n+1} is connected to no vertex in V_1. Hence

$\{V_1, V_2 \cup \{v_{n+1}\}\}$ gives a non-trivial partition of $V_Q - \{v_t\}$ and it moreover splits G_Q. Now from how we are viewing G being reducible we know $1 = \gcd\{r_i : v_i \in V_1\}$, $1 = \gcd\{r_i : v_i \in V_2\}$, and

$$r_t \mid \sum_{j \in J} M_{t,j} r_j.$$

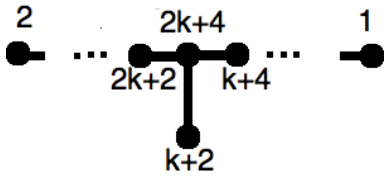
where $J := \{j : M_{t,j} \neq 0\} \cap V_1$. Note that by what we showed above and by the way blow-ups are constructed we have $J = \{j : M_{Q_{t,j}} \neq 0\} \cap V_1$. From all these it is clear now that G_Q is indeed reducible at v_t with the above choice of partition of $V_Q - \{v_t\}$. $\square$

Chapter 9

irreducible arithmetical trees of g-integer 0

It is easy to see that for an arbitrary arithmetical graph we have $g(M) = 0$ if and only if $\phi(M) = 1$ and $\rho(M) = 0$. The question still remains as to what values of $g_0(M)$ can occur for the graphs with $g(M) = 0$. The following family of examples shows that every possible value of $g_0(M)$ will occur.

Example 9.1. Here $-1 \leq k$ is an arbitrary odd integer. We then have:



Here we use Euclid's Lemma (Remark 4.2 in [Lor1]) to construct the non-trivial terminal chains (if $k = -1$ then we make these two chains start out with vertices of multiplicity 1 and 2). We see that:

(a) G is an irreducible tree

(b) $\phi(M) = 1$

(c) $\rho(M) = 0$

(d) $g_0(M) = \frac{k+1}{2}$

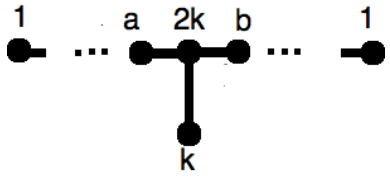
(e) $g(M) = 0$.

Chapter 10

Irreducible arithmetical trees of g-integer 1

It is easy to see that for an arbitrary arithmetical graph we have $g(M) = 1$ only if $2 \leq \phi(M)$ and $\rho(M) = 0$. Note that the converse is false, however. The question still remains as to what values of $\phi(M)$ and $g_0(M)$ can occur for the graphs with $g(M) = 1$. The following family of examples shows that for $\phi(M) = 2$ we have that every possible value of $g_0(M)$ will occur.

Example 10.1. Let k be an arbitrary even positive integer. If a, b are any positive integers, each of which is coprime to k, and with either $a+b = k$ or $a+b = 3k$ holding, then consider:



Here we use Euclid's Lemma (see Remark 4.2 in [Lor1]) to construct the two non-trivial terminal chains. We see that:

(a) G is an irreducible tree

(b) $\phi(M) = 2$

(c) $\rho(M) = 0$

(d) $g_0(M) = \frac{k}{2}$.

If the two multiplicity 1 vertices determined the same class then we see, by Proposition 2.7 in [Lor4], that there would be the only one degree $\frac{k}{2}$ class represented by an effective. This would create a contradiction as $g(M) \leq g_0(M) = \frac{k}{2}$. Thus they determine different classes, so it is clear that $g(M) = 1$.

Proposition 10.2. *Let s be a non-negative integer and put*

$$D_s := \{r \in \mathbb{Z} : r \text{ is the degree of a vertex of a minimal arithmetical graph of } g\text{-integer } s\}.$$

It follows that D_s is an infinite set.

Proof : For any even positive integer k let G_k be the graph in the Example 10.1 that corresponds to the same k and where $a + b = k$. For $s \neq 0$ consider the arithmetical graph we get when we start with G_k and then join to it, at one of its vertices of multiplicity 1, $s-1$ copies of G_k, each at a multiplicity 1 vertex. By Proposition 7.4 we see that the resulting graph has g-integer equal to s. Further, it is clear that this graph is minimal. Finally, if $k' \neq k$ then $G_{k'}$ is not similar to (see 1.5 in [A-W]) G_k. Since k was arbitrary we indeed get D_s being infinite. When $s = 0$ take for any odd positive integer k the graph in Example 9.1, yielding that D_0 is infinite. □

Remark 10.3. Proposition 10.2 shows that no case of Theorem 1.6 nor even Corollary 1.7 in [A-W] is true if we replace their genus of type by our g-integer.

In the rest of this chapter we make use of the following two concepts.

Definition 10.4. Let $t(M)$ denote the number of multiplicity 1 vertices.

10.5. For an arithmetical tree (G, M, R) and a non-terminal vertex v_1 that disconnects G we can perform what is called a *break and complete*. First we break G at v into two graphs. Let $X_1 := \{v_2, ..., v_k\}$ and $X_2 := \{v_{k+1}, ..., v_\ell\}$ be a non-trivial partition of the vertices of G that are connected to v_1. Let G_i be the subgraph of G on the vertices $\{v_j \in V_G$: the path from v_1 to v_j goes through some vertex in $X_i\} \cup \{v_1\}$. Put $h_i :=$gcd{the multiplicities of the vertices in G_i}. Complete G_1 (resp. G_2) into an arithmetical tree by first replacing for all v_j in V_{G_1} (resp. in V_{G_2}) r_j by r_j/h_1 (resp. by r_j/h_2), second by attaching a single new vertex v_* (resp. v^*) to v_1 of multiplicity $r_* := \sum_{j=k+1}^{\ell} \frac{r_j}{h_1}$ (resp. $r^* := \sum_{j=1}^{k} \frac{r_j}{h_2}$), and then finally using Euclid's lemma to form a terminal chain with $(v_1,\ r/h_1)$ and (v_*, r_*) (resp. $(v_1,\ r/h_2)$ and (v^*, r^*)), ending in a vertex v_{s_1} (resp. v_{s_2}). We see that $h_1 \cdot r_{s_1} = h_2 \cdot r_{s_2}$. Denote this common value by ω.

Proposition 10.6. *Let G be an irreducible tree. If $\phi(M) \leq t(M)$ then $2^{t(M)-2} \leq \phi(M)$.*

Proof : Suppose $\phi(M) \leq t(M)$. If G has no nodes then we are immediately done. Suppose G has at least one node. We note that, by irreducibility of G, we know that a vertex has multiplicity 1 only when the vertex is terminal. By abuse of notation we write the nodes of G as

$$v_1, ..., v_\ell.$$

We let d_i denote the degree of v_i. When v_i has at least one terminal chain attached to it we will let

$$v_{i_1}, ..., v_{i_{k_i}}$$

be the terminal vertices of G associated to v_i.

We will show, by induction on ℓ, that

$$2^{t(M)-2} \leq \phi(M).$$

First, suppose $\ell = 1$. If $t(M) = 1$ then we are done. Assume that $2 \leq t(M)$. We have

$$\phi(M) = \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}}$$

and $d_1 = k_1$. Then, since $2 \leq t(M)$, $1 \leq \frac{r_1}{r_{1_j}}$, and $2 \leq \frac{r_1}{1}$ we have

$$2^{t(M)-2} \leq \phi(M).$$

Now suppose that $2 \leq \ell$. Suppose further that $2^{t(M_0)-2} \leq \phi(M_0)$ for all irreducible arithmetical trees that satisfy $\phi(M_0) \leq t(M_0)$ and whose number of nodes is in $\{1, ..., \ell - 1\}$. Choose a terminal node of G, say v_1, such that not all of the multiplicity one vertices of G are on the terminal chains attached to v_1. Let v_* be the vertex adjacent to v_1 on the unique connecting chain attached to v_1. We break G at v_* in this manner. We then complete it as in 10.5. Let G_1 denote the completion of $G - (C - v_*)$. Write the vertices, from v_* to the terminal vertex, of terminal chain in order:

$$(v_*, v_{\epsilon_1}, ..., v_{\epsilon_s}).$$

We choose, as we can, to have the multiplicity of v_{ϵ_1} equal to r_1, the multiplicity of v_1.

Put $\omega_1 :=\gcd(r_{1_1}, ..., r_{1_{k_1}})$. We know that $\frac{r_1^{d_1-2} \cdot \omega_1}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}}$ is a positive integer. and also that ω_1 divides both r_1 and r_*. Thus, in addition we get $\omega_1 | r_{\epsilon_j}$ for all $j \in \{2, ..., s\}$. Consequently,

$$\gcd(C) \mid \gcd(r_*, r_{\epsilon_1}, ..., r_{\epsilon_s}).$$

Thus, by G being irreducible, it is immediate that the only place at which we can possibly make G_1 reducible is at a vertex in $V := \{v_{\epsilon_1}, ..., v_{\epsilon_s}\}$.

Now, since $r_{\epsilon_{i+1}} < r_{\epsilon_i}$ for any $i \in \{1, .., s-1\}$ we see that G_1 can not be made reducible at any vertex in V. Thus, G_1 is irreducible. Clearly G_1 is a tree. By construction, G_1 has exactly one fewer node than G does. Let $t(M_1)$ be defined to be the number of multiplicity 1 vertices in G_1. Let $t(M^{'})$ denote the number of multiplicity 1 vertices in $G - C$. Thus, $t(M_1) = t(M^{'})$ if $r_{\epsilon_s} \neq 1$, while $t(M_1) = t(M^{'}) + 1$ if $r_{\epsilon_s} = 1$. Now, let us show that $\phi(M_1) \leq t(M_1)$. We note that

$$\phi(M) = \phi(M_1) \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}} \cdot r_{\epsilon_s} \qquad (*)$$

We know that $\frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}} \cdot r_{\epsilon_s}$ is an integer since it is clear that $\frac{r_1^{d_1-2} \cdot \omega_1}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}}$ and $\frac{r_{\epsilon_s}}{\omega_1}$ are each integers. Put $p := t(M) - t(M^{'})$. If $p = 0$ then

$$\phi(M_1) = \frac{\phi(M)}{r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}}} \leq \phi(M) \leq t(M) = t(M^{'}) \leq t(M_1).$$

Now suppose $1 \leq p$. Thus,

$$r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}} = r_{\epsilon_s} \cdot r_i^{p-1} \cdot \frac{r_1}{r_{1_{p+1}}} \cdot \ ... \ \cdot \frac{r_1}{r_{1_{k_1}}}$$

where $p \leq k_1$. Hence,

$$2^{p-1} \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}} \qquad (**)$$

and if $2 \leq r_{\epsilon_s}$ then moreover

$$2^p \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}} \qquad (***).$$

Thus,

$$\phi(M_1) = \frac{\phi(M)}{r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot ... \cdot r_{1_{k_1}}}} \leq \begin{cases} \frac{\phi(M)}{2^{p-1}} & \text{if } r_{\epsilon_s} = 1 \\ \frac{\phi(M)}{2^p} & \text{if } 2 \leq r_{\epsilon_s} \end{cases}$$

Thus, as $1 \leq \frac{\phi(M)}{2^{p-1}}$, we know

$$\frac{\phi(M)}{2^{p-1}} \leq \phi(M) - (p-1) \leq t(M) - (p-1) = t(M) - p + 1 = t(M^{'}) + 1,$$

and so if $r_{\epsilon_s} = 1$ then $\frac{\phi(M)}{2^{p-1}} \leq t(M^{'}) + 1 = t(M_1)$. If $2 \leq r_{\epsilon_s}$ then $1 \leq \frac{\phi(M)}{2^p}$ and hence we have

$$\frac{\phi(M)}{2^p} \leq \phi(M) - p \leq t(M) - p = t(M^{'}) = t(M_1).$$

Thus, no matter what the value of p is we must always have $\phi(M_1) \leq t(M_1)$. Hence, by the inductive hypothesis, we get $2^{t(M_1)-2} \leq \phi(M_1)$. Thus, based upon how we write $\phi(M)$ in $(*)$ we see that we get $2^{t(M)-2} \leq \phi(M)$ if we can show somehow that

$$2^{t(M)-t(M_1)} \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot \ldots \cdot r_{1_{k_1}}}.$$

If $2 \leq r_{\epsilon_s}$ then $p = t(M) - t(M_1)$ and so, when $p \neq 0$, $(**)$ above gives that

$$2^{t(M)-t(M_1)} = 2^{p-1} \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot \ldots \cdot r_{1_{k_1}}}.$$

If $r_{\epsilon_s} = 1$ then $p - 1 = t(M) - t(M_1)$ and so, when $p \neq 0$, $(***)$ gives

$$2^{t(M)-t(M_1)} = 2^p \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot \ldots \cdot r_{1_{k_1}}}.$$

Finally, if $p = 0$ then $t(M) - t(M_1) \leq 0$ and we trivially get

$$2^{t(M)-t(M_1)} \leq r_{\epsilon_s} \cdot \frac{r_1^{d_1-2}}{r_{1_1} \cdot \ldots \cdot r_{1_{k_1}}}.$$

□

We then obtain the following corollary.

Corollary 10.7. *Let G be an irreducible tree with $\phi(M) \leq t(M)$. Then $\phi(M) \leq 3$.*

Proof : Since $2^{t(M)-2} \leq \phi(M)$ by Proposition 10.6, we get $2^{t(M)-2} \leq t(M)$, making $t(M)$, and hence $\phi(M)$, at most 4.

Suppose now that $\phi(M) = 4$. By Prop 10.6 we get $t(M) = 4$. We first see that G must have more than one node (it clearly must have at least one node, unless $\phi(M) = 1$) for if it had exactly one node then

$$\phi(M) = \frac{r_1}{r_{1_1}} \cdot \frac{r}{r_{1_2}} \cdot \ldots \cdot \frac{r}{r_{1_{d-4}}} \cdot r_1^2$$

with $d \geq 4$. This makes $r_1 = 2$ and $r_{1_i} = 2$ if $1_i \in \{1, \ldots, d-4\}$. But then G is clearly reducible.

Form G_1 as in Proposition 10.6. We can then inductively assume that $\phi(M_1) \neq 4$. Thus $\phi(M_1) \in \{1, 2\}$. If $\phi(M_1) = 1$ and $r_{\epsilon_s} = 1$ then $t(M_1) = 2$, making $t(M) = 3$. But then $4 = \frac{r_1}{r_{1_1}} \cdot \frac{r_1}{r_{1_2}} \cdot \ldots \cdot \frac{r}{r_{1_{d-4}}} \cdot r_1^2$, so $r_1 = 2$ and we see that G is reducible. If $\phi(M_1) = 1$ and $r_{\epsilon_s} \neq 1$ then $t(M_1) = 1$ (and $t(M) = 3$) or $t(M_1) = 2$ (and $t(M) = 2$). In the former we see that $r_1^2 \cdot r_{\epsilon_s}$ divides 4, a contradiction. In the latter case we get that $r_1 = 2$, and hence that G is reducible. Therefore, $\phi(M_1) = 2$ must hold. If $r_{\epsilon_s} = 1$ then $t(M_1) = 2$ (and $t(M) = 3$) or

$t(M_1) = 3$ (and $t(M) = 2$). In the former we get r_1^2 dividing 2. In the latter we get $r_1 = 2$ and hence G being reducible. If, instead, $r_{\epsilon_s} \neq 1$ then either $t(M_1) = 1$ (and $t(M) = 3$) or $t(M_1) = 2$ (and $t(M) = 2$) or $t(M_1) = 3$ (and $t(M) = 1$). If $t(M) = 3$ or $t(M) = 2$ then $r_1 \cdot r_{\epsilon_s}$ divides 2, a contradiction. If $t(M) = 1$ then $r_{\epsilon_s} = 2$ and all but one terminal vertex associated to v_1 has multiplicity equal to r_1. Since the other terminal vertex is 1 we find that $r_{\epsilon_s} = 1$ must hold, a contradiction. Thus $\phi(M) \neq 4$ indeed holds, as claimed. □

Remark 10.8. Proposition 10.6 always applies to an irreducible arithmetical tree of g-integer 1. The reason is because there must be $\phi(M)$ degree 1 classes represented by an effective divisor, and any such divisors naturally corresponds to vertices of multiplicity 1.

Remark 10.9. We recall that there is a specific important pairing on the component group (see 3.1 in [Lor4] for its definition):

$$\Phi(M) \times \Phi(M) \to \mathbb{Q}/\mathbb{Z}.$$

It is a useful tool in determining the g-integer in certain situations.

Proposition 10.10. *If G is an irreducible tree with $g(M) = 1$ and $\phi(M) = 2$ then $t(M) = 2$.*

Proof : If $t(M) \neq 2$ then $t(M) = 3$. If G has exactly one node then, as $\phi(M) = 2$, we see that the multiplicity of the node is 2 and that $4 \leq t(M)$, a contradiction. Thus we can and do assume that G has at least two nodes. We will complete the proof by induction on the number of nodes. Form G_1 as in Proposition 10.6.

First suppose that $\phi(M_1) = 1$. If $r_{\epsilon_s} = 1$ then $t(M_1) = 2$ so $t(M) = 2$, making $r_1 = 2$. As $r_1 = 2$ we must have an even number of adjacent chains of weight 1, a contradiction. If on the other hand $r_{\epsilon_s} \neq 1$ then $t(M_1) = 1$ (so $t(M) = 2$) or $t(M_1) = 2$ (so $t(M) = 1$). In the former case $r_{\epsilon_s} \cdot r_1$ divides 2, a contradiction. In the latter case $r_{\epsilon_s} = 2$, yielding, along with $t(M) = 1$, that exactly one adjacent chain has weight relatively prime to r_1, a contradiction.

Now suppose that $\phi(M_1) \neq 2$. If $r_{\epsilon_s} = 1$ then $t(M_1) = 2$ (so $t(M) = 2$) or $t(M_1) = 3$ (so $t(M) = 1$). In the former case we must have then that r_1 divides 1. In the latter case we can blow-down all the terminal chains ending in r_1, yielding an irreducible tree with one fewer node than G. The component group is still of order 2 and there are still exactly three multiplicity one vertices. If we take the two multiplicity 1 vertices of G that are not associated to the node used in making G_1 then these same vertices in this new tree are still distinct in light of pairing the difference of these two vertices with itself (as in Proposition

3.2 in [Lor4]) along with the fact that the component group of G is of prime order. If $r_{\epsilon_s} \neq 1$ then $t(M_1) = 2$ (so $t(M) = 1$) or $t(M_1) = 3$ (so $t(M) = 0$). In the former all but exactly one weight of an adjacent chain is relatively prime to r_1, a contradiction. In the latter $G^{'}$ violates the inductive hypothesis because the two multiplicity 1 vertices in G that are distinct remain distinct in G_1, in light of the pairing (see prop. 3.2 in [Lor4]). □

Corollary 10.11. *If G is a tree with $g(M) = 1$ then $\phi(M) \leq 4$.*

Proof : Suppose G is a tree with $g(M) = 1$. If G is irreducible then we are done in light of the Corollary 10.7 and Remark 10.8. Suppose that G is reducible. Thus, we have

$$G = ((...((G_1 \oplus G_2) \oplus G_3) \oplus ...) \oplus G_k)$$

where $2 \leq k$, each G_i is irreducible, and each join is a simple join. Since $g(M) = 1$ we use Proposition 7.4 and Corollary 7.7 and find that one of the two following collections of facts holds. The first is that each G_i has g-integer 0, and that of all the multiplicities of the vertices at which the $k-1$ joins take place there is exactly one of them of multiplicity equal to 2 with all the other multiplicities being equal to 1. The second is that exactly one G_i will have g-integer 1 with the all the rest having g-integer 0, and that the multiplicities of the vertices at which the $k-1$ joins take place are all equal to 1.

The next two facts are easily seen to hold due to Proposition 7.9, along with the fact that an arithmetical graph of g-integer 0 has its component group having order 1.

If $G^{'}$ and $G^{''}$ are trees, one of which has g-integer 0 and the other g-integer 1, then at any simple join, $G^{'} \oplus G^{''}$, where the associated multiplicity equals 1 we have

$$\phi(M^{'} \oplus M^{''}) = \phi(M^{'}) \cdot \phi(M^{''}) \cdot 1^2 \in \{\phi(M^{'}), \phi(M^{''})\}.$$

If $G^{'}$ and $G^{''}$ are trees of g-integer 0 then at any simple join, $G^{'} \oplus G^{''}$, of multiplicity 2 we have

$$\phi(M^{'} \oplus M^{''}) = \phi(M^{'}) \cdot \phi(M^{''}) \cdot 2^2 = 4.$$

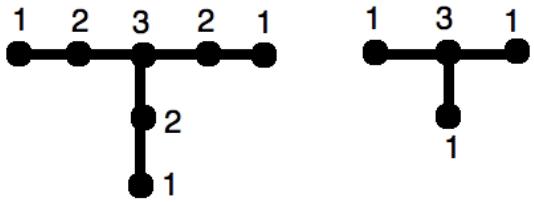
These two facts, along with the fact that $\phi(M_i) \leq 4$, by Corollary 10.7 along with Remark 10.8, and the fact the operation of join is commutative, yield

$$\phi(M_1 \oplus M_2 \oplus ... \oplus M_k) \leq 4,$$

as desired. □

The following example contains two important arithmetical trees. We note that both have g-integer 1.

Example 10.12.



10.13. Let (G, M, R) be an irreducible arithmetical tree. If there is a vertex v_i that is not a node and is such that $M_{i,i} = 1$ we blow it down to get another arithmetical tree, say (G', M', R'). This is irreducible (by Proposition 8.5), and has $g(M') = 1$ (by Proposition 8.1). If the new tree then has a vertex v_j' that is not a node with $M'_{j,j} = 1$, then we repeat the process. We continue to repeat it until then are no more such vertices (that are not nodes) to blow-down.

Proposition 10.14. *Let (G, M, R) be an irreducible arithmetical tree of g-integer 1 having exactly one node. After applying the process described in 10.13 we get an arithmetical tree isomorphic to a tree in either Example 10.1 or Example 10.12.*

Proof : Let (G', M', R') be the arithmetical tree resulting from 10.13. This has a single node. Let r' denote the multiplicity of this node. We know that $\phi(M') \neq 1$ since $g(M') \neq 0$. Hence, $\phi(M')$ is 2 or 3 (by Corollary 10.7). Further at least two vertices have multiplicity 1 by Remark 10.8. Moreover, any such vertex is terminal by irreducibility. Hence, by the formula for the order of the component group of a tree we see that there is a terminal chain ending in $\frac{r}{2}$ (in case $\phi(M') = 2$) or $\frac{r}{3}$ (in case $\phi(M') = 3$), with all other chains, except those ending in 1, ending in r. But there cannot be any chains (by 10.13) ending in r because then on that chain there would be a vertex v_i' (that is not a node) with $M'_{i,i} = 1$. Thus (G', M', R') has exactly three terminal chains. If $\phi(M') = 2$ then exactly two terminal chains end in 1, and we see that this is a tree in Example 10.1. On the other hand, if $\phi(M) = 3$ then $g(M) = 1$ forces each chain to end in 1 and $r = 3$. We are clearly have one of the trees in Example 10.12. □

Corollary 10.15. *The number of non-isomorphic irreducible trees having exactly one node and exactly three terminal chains of g-integer 1 and linear rank s is 5 if $s = 1$, $\frac{3}{2} \cdot \phi(s)$ if $s \neq 1$ is odd, and $3 \cdot \phi(s)$ if s is even (here ϕ denotes the Euler totient function).*

Proof : If $s = 1$ then we have three such trees from Example 10.1 and two from Example 10.12. For $s \neq 1$ The trees in Example 10.1 with $2s = k$ provide all of the examples. The ones where the node has self-intersection $M_{i,i}$ equal to 1 (resp. 2) number $\frac{\phi(k)}{2}$ (resp. $\frac{\phi(2k)}{2}$). The total number is $\frac{\phi(k)+\phi(2k)}{2} = \frac{\phi(2s)+\phi(4s)}{2}$. If s is odd (resp. even) then this number is $\frac{\phi(s)+2\phi(s)}{2}$ (resp. $\frac{2\phi(s)+4\phi(s)}{2}$). □

Proposition 10.16. *If G is an irreducible tree with $g(M) = 1$ and $\phi(M) = 2$ then we can naturally associate to G simpler arithmetical trees. Namely, by repeatedly breaking and completing G (as in 10.5), we get a collection of irreducible trees $G_1, G_2, ..., G_k$, each with only one node. We can construct the $G_1, G_2, ..., G_k$ so that each has exactly two multiplicity 1 vertices, with both such vertices terminal and associated to the same node. Moreover, we can additionally take these trees so that G_1 has g-integer 1 and each other G_i has g-integer 0.*

Proof : If G has exactly one node then we are done by Proposition 10.10. Suppose G has more than one node. We know that G itself has exactly two multiplicity 1 vertices, with both being terminal by irreducibility. If the two vertices happen to be associated to the same node then break G at that node so that the two terminal chains form one piece. Otherwise, break G along any connecting chain on the unique path between these two vertices. In either case, complete each piece into an arithmetical graph. If we let ω be the weight of such a chain then

$$\phi(M) = \phi(M_1) \cdot \phi(M_2) \cdot \omega^2$$

making $\phi(M_1) = 2$ and $\phi(M_2) = 1$. Thus $g(M_2) = 0$ clearly. Now since the above formula forces $\omega = 1$ we see that there are two multiplicity 1 vertices on G_1. The difference of these two vertices is non-zero in $\Phi(M_1)$ since if it were not then we get a contradiction using the pairing (see 10.9) on G. This is accomplished by observing that the difference of the two multiplicity 1 vertices in G_2 is zero in $\Phi(M_2)$. We see that taking the difference of the two multiplicity 1 vertices in G and pairing it with itself yields an integer, which is equal to the sum of the the analogous representatives in G_1 and G_2 plus an additional sum. But this additional sum is an integer, since it is the pairing applied to the difference of a pair of vertices on a tree with no nodes paired with itself. For each of the two resulting arithmetical trees we can, if needed, cut and complete again until we get what is claimed. □

Proposition 10.17. *If G is an irreducible tree with $g(M) = 1$ and $\phi(M) = 3$ then we can naturally associate to G simpler arithmetical trees. Namely, by repeatedly breaking and completing G (as in 10.5), we get a collection of irreducible trees $G_1, G_2, ..., G_k$, each with only one node. We can construct the $G_1, G_2, ..., G_k$ so that each has exactly three multiplicity 1 vertices, with all three such vertices terminal and associated to the same node. Moreover, we can additionally take these trees so that G_1 has g-integer 1 with $\phi(M_1) = 3$ and each other G_i has g-integer 0.*

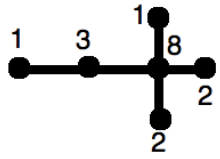
Proof : The proof is similar to that of the Proposition 10.16, in that we cut and complete in the same manner until we reach our desired results. □

Chapter 11

Existence of a canonical divisor

If G is reduced, or more generally if $g(M) = g_0(M)$ then G has a canonical divisor (see Proposition 4.2(b) in [Lor2]). It is not true, however, that there is always a canonical divisor, as the next example shows.

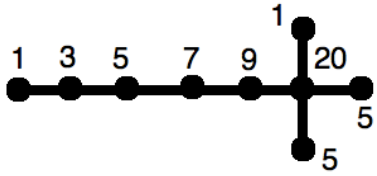
Example 11.1.



Here we have $g_0(M) = 6$ and $g(M) = 5$, yet no canonical divisor. We have $\Phi(M) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We note that of the 16=$\phi(M)$ divisor classes of degree 4=$g(M) - 1$ exactly twelve are represented by an effective. See Appendix C for these computations.

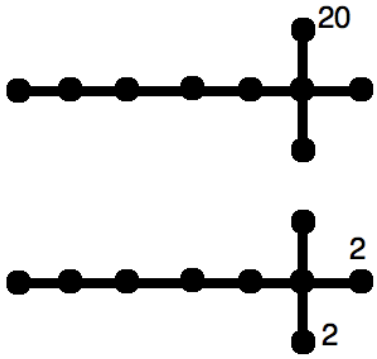
On the other hand it is possible to have more than one canonical class.

Example 11.2.



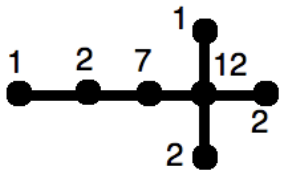
In this example we have $g(M) = 11$ while $g_0(M) = 15$. We have $\Phi(M) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and there are exactly two degree 10 divisor classes not represented by an effective, say A and B. We then see that $A + B$ has to be a canonical divisor. Since a canonical divisor in this

example is determined by its action on $\{A, B\}$, we know there is at most one more possible canonical class, namely $[2A]$. We observe that $2A$ will be a canonical divisor if and only if $2A \sim 2B$. By using the program in Appendix C we find that there are indeed two canonical classes, so $2A \sim 2B$ in particular, must hold. The canonical classes have the following degree 20 divisors as representatives:

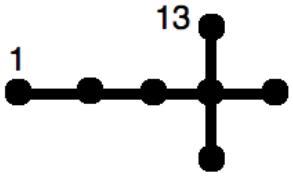


We noted above that a canonical exists whenever $g(M) = g_0(M)$. Also, there will always be one as long as either $\phi(M) \leq 5$ or the number of degree $g(M) - 1$ divisor classes not represented by an effective is at most 2 or at least $\phi(M) - 2$. An example where a canonical divisor exists yet none of the above hold is:

Example 11.3.



Here $g(M) = 8, g_0(M) = 10$, $\Phi(M) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and there are exactly 30 degree 7 classes represented by an effective. It turns out that there is exactly one canonical class. An explicit representative of this class is the following degree 14 divisor (see Appendix C for all these computations):



Chapter 12

Computations for modular curves

Let $p \geq 5$ be a prime and consider the modular curve $X_0(p^2)/\mathbb{Q}_p^{unr}$. The associated intersection matrix M for its minimal regular model is found in 1.5 of [Edi1]. It is shown in [Edi2] that $\Phi(M)$ is cyclic of order $\frac{p^2-1}{24}$.

Proposition 12.1. *We have* $g(M) = \phi(M) - 1$.

Proof : If $p = 12k+1$ then M is the matrix

$$\begin{pmatrix} 1 & -1 & -1 & -k & -k \\ -1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 3 & 0 & 0 \\ -k & 0 & 0 & kp & -k \\ -k & 0 & 0 & -k & kp \end{pmatrix}$$

and $R = (p-1, (p-1)/2, (p-1)/3, 1, 1)^t$. One then checks directly that

$$M \cdot (12k-6, 6k-3, 4k-2, 1, 1)^t = (-1, 0, 0, 6k, 6k)^t$$
$$M \cdot (12k-3, 6k-2, 4k-1, 1, 1)^t = (0, -1, 0, 3k, 3k)^t$$
$$M \cdot (12k-2, 6k-1, 4k-1, 1, 1)^t = (0, 0, -1, 2k, 2k)^t.$$

This has two important consequences. The first is that every degree 0 divisor is equivalent to one of the form $(0, 0, 0, a, -a)^t$, and hence, since $\Phi(M)$ is cyclic, the class of $(0, 0, 0, 1, -1)^t$ generates the component group. The other consequence is that every effective divisor is equivalent to an effective divisor supported only possibly at the multiplicity 1 vertices. Putting these together we see that there are exactly $\phi(M) - s + 1$ effective classes of degree $\phi(M) - s$ for $s \in \{1, 2, ..., \phi(M)\}$. Therefore, $g(M) = \phi(M) - 1$.

The three other cases $p = 12k+5, p = 12k+7, p = 12k+11$ are similar. In the first case M is

$$\begin{pmatrix} 1 & -1 & -1 & -k & -k \\ -1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 3 & -1 & -1 \\ -k & 0 & -1 & kp+(p+1)/3 & -k \\ -k & 0 & -1 & -k & kp+(p+1)/3 \end{pmatrix}$$

and $R = (p-1, (p-1)/2, (p+1)/3, 1, 1)^t$ with

$$\begin{aligned} M \cdot (12k-2, 6k-1, 4k, 1, 1)^t &= (-1, 0, 0, 6k+2, 6k+2)^t \\ M \cdot (12k+1, 6k, 4k+1, 1, 1)^t &= (0, -1, 0, 3k+1, 3k+1)^t \\ M \cdot (12k+2, 6k+1, 4k+1, 1, 1)^t &= (0, 0, -1, 2k+1, 2k+1)^t. \end{aligned}$$

In the second case we have that M is

$$\begin{pmatrix} 1 & -1 & -1 & -k & -k \\ -1 & 3 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & -1 \\ -k & 0 & -1 & kp+(p+1)/2 & -k \\ -k & 0 & -1 & -k & kp+(p+1)/2 \end{pmatrix}$$

and $R = (p-1, (p-1)/3, (p+1)/2, 1, 1)^t$ with

$$\begin{aligned} M \cdot (12k, 4k, 6k+1, 1, 1)^t &= (-1, 0, 0, 6k+3, 6k+3)^t \\ M \cdot (12k+4, 4k+1, 6k+3, 1, 1)^t &= (0, -1, 0, 2k+1, 2k+1)^t \\ M \cdot (12k+3, 4k+1, 6k+2, 1, 1)^t &= (0, 0, -1, 3k+2, 3k+2)^t. \end{aligned}$$

In the last case M is

$$\begin{pmatrix} 1 & -1 & -1 & -k & -k \\ -1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 3 & -1 & -1 \\ -k & 0 & -1 & kp+(5p+5)/6 & -k \\ -k & 0 & -1 & -k & kp+(5p+5)/6 \end{pmatrix}$$

and $R = (p-1, (p+1)/2, (p+1)/3, 1, 1)^t$ with

$$\begin{aligned} M \cdot (12k+4, 6k+3, 4k+2, 1, 1)^t &= (-1, 0, 0, 5k+5, 5k+5)^t \\ M \cdot (12k+7, 6k+4, 4k+3, 1, 1)^t &= (0, -1, 0, 3k+3, 3k+3)^t \\ M \cdot (12k+7, 6k+4, 4k+3, 1, 1)^t &= (0, 0, -1, 2k+2, 2k+2)^t. \end{aligned}$$

For the same reasons we get in these three cases too that $g(M) = \phi(M) - 1$. □

Corollary 12.2. *G has exactly one canonical class.*

Proof : This holds since, by the Proposition 12.1, there are exactly $\phi(M) - 1$ effective classes of degree $g(M) - 1$. An explicit canonical divisor is (0,0,0,-2,$2 \cdot \phi(M) - 2)^t = 2 \cdot (0, 0, 0, -1, \phi(M) - 1)^t$. To verify this one simply checks the degree $g(M) - 1$ divisor $(0, 0, 0, -1, \phi(M) - 1)^t$ is not equivalent to an effective. If it were equivalent to an effective then $(0, 0, 0, 1, -1)^t$ would not generate all of $\Phi(M)$. □

Chapter 13

Bounding $\phi(M)$ in terms of the g-integer

In this chapter we assume throughout that our arithmetical graph (G, M, R) is in fact an arithmetical tree.

Definition 13.1. For a positive integer $x = p_1^{a_i} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$ let $\ell(x) := \Sigma(a_i - 1) \cdot p_i$.

13.2. From Theorem 2.4 in [Lor3] we have

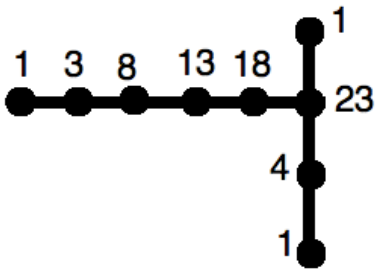
$$\ell(\phi(M)) \leq 2 \cdot g_0(M).$$

13.3. As a corollary to 13.2 we have

$$\phi(M) \leq 4^{g_0(M)}.$$

It turns out that 13.2 does not hold if we replace $g_0(M)$ by $g(M)$, as the next example shows.

Example 13.4.



One checks using Appendix C that $g(M) = 7$. But $\phi(M) = 23$, making $\ell(\phi(M)) = 22$.

13.5. The analogue of 13.3 is, however, not settled. It may be that the inequality

$$\phi(M) \leq 4^{g(M)}$$

holds for all arithmetical trees.

We now present three cases where it is satisfied.

Proposition 13.6. *Suppose that G has exactly one node and exactly three terminal chains. Further suppose $\phi(M) \neq 1$. It then follows that $\lfloor \sqrt{\phi(M)} \rfloor \leq g(M)$.*

Proof : We show that the number of degree $\xi := \lfloor \sqrt{\phi(M)} \rfloor - 1$ equivalence classes that are represented by an effective divisor is less than $\phi(M)$. We note first that any effective divisor can be represented by an effective divisor whose support is a subset of the terminal vertices. This holds by Proposition 2.7 and Proposition 3.4 in [Lor4]. These say that if r_i and r_j are the multiplicities of two different vertices on the same terminal chain, with the second vertex terminal, then the vector with $\frac{r_i}{r_j}$ in the component for the terminal vertex, -1 in the component for the other vertex, and 0 elsewhere, is in $\mathrm{im}(M)$. Hence, they allow us to take our arbitrary effective divisor and add to it divisors of the above shape yielding ultimately an effective divisor with 0 in every component except possibly the components of the terminal vertices.

Let v_1, v_2, v_3 denote the three terminal vertices, with r_1, r_2, r_3 as their respective multiplicities.

We are thus reduced to counting the number of degree ξ effective divisors with the above type of support. Let c_1, c_2, c_3 be the values of such a divisor at the three terminal vertices. Thus,

$$r_1c_1 + r_2c_2 + r_3c_3 = \xi - 1. \ (*)$$

Thus, $0 \leq c_1 \leq \xi - 1$ and $0 \leq c_2 \leq \xi - 1 - c_1$. Moreover, for any c_1, c_2 within the above parameters there is at most one non-negative c_3 making (*) hold. Now the number of such (c_1, c_2, c_3) is at most $1 + 2 + ... + \xi + (\xi + 1) = \frac{(\xi+1)\cdot(\xi+2)}{2} = \frac{(\lfloor\sqrt{\phi(M)}\rfloor)\cdot(\lfloor\sqrt{\phi(M)}+1\rfloor)}{2} = \frac{\lfloor\sqrt{\phi(M)}\rfloor^2+\lfloor\sqrt{\phi(M)}\rfloor}{2}$. One easily checks, since $\phi(M) \neq 1$, that this is less than $\phi(M)$. □

Corollary 13.7. *Under the hypotheses of Lemma 13.6 we have that $\phi(M) \leq 4^{g(M)}$.*

Proof : Since $\lfloor \sqrt{\phi(M)} \rfloor \leq g(M)$ we get $\phi(M) \leq (g(M) + 1)^2$. As $(g(M) + 1)^2 \leq 4^{g(M)}$ whenever $0 < g(M)$ the proof is complete. □

Proposition 13.8. *If $g(M) \leq 1$ then $\phi(M) \leq 4^{g(M)}$.*

Proof : This was shown for $g(M) = 1$ in 10.11. If $g(M) = 0$ then $\phi(M) = 1$ and we have the inequality in this case too. □

Lemma 13.9. *If a, b, c are positive integers with gcd(a, b)=1, $a|c$, and $b|c$ then we have $\frac{c}{a \cdot b} \leq 2^{1+c-(a+b)}$.*

Proof : Put $\alpha := \frac{c}{a \cdot b}$. One easily checks that, provided at most one of α, b, c equals 1,

$$-1 \leq \alpha \cdot b \cdot c - b - c - \alpha,$$

equivalently, $\frac{a}{b \cdot c} \leq 1 + a - (b + c)$. If $\alpha = 1$ we already have what we want to show. If $2 \leq \alpha$ and $b, c = 1$ then we are trying to see whether $\alpha \leq 2^{\alpha - 1}$ holds, which clearly does. □

Proposition 13.10. *Let (G'', M'', R'') be the join of (G, M, R) and (G', M', R'). If $\phi(M) \leq 4^{g(M)}$ and $\phi(M') \leq 4^{g(M')}$ then $\phi(M'') \leq 4^{g(M'')}$.*

Proof : By Proposition 7.4 and Proposition 7.9, we see its enough to show

$$\phi(M) \cdot \phi(M') \cdot \frac{r_n \cdot r_1'}{h' \cdot h} \leq 4^{h \cdot (g(M)-1) + h' \cdot (g(M')-1) + r + 1}.$$

As $\phi(M_i) \leq 4^{g(M_i)}$, we see that all we have to show is

$$\frac{r_n \cdot r_1'}{h' \cdot h} \leq 4^{h_1 \cdot (g(M_1)-1) + h_2 \cdot (g(M_2)-1) + \omega + 1 - g(M_1) - g(M_2)}.$$

Recall that $r = r_n \cdot h = r_1' \cdot h$. Thus, $\frac{r_n \cdot r_1'}{h' \cdot h} = \frac{r \cdot r}{h \cdot h' \cdot h \cdot h'}$, making $\sqrt{\frac{r_n \cdot r_1'}{h' \cdot h}} = \frac{r}{h \cdot h'}$. This along with the fact that

$$1 + \omega - h - h' \leq h \cdot (g(M_1) - 1) + h' \cdot (g(M_2) - 1) + \omega + 1 - g(M_1) - g(M_2).$$

tells us that it is sufficient to show

$$\frac{\omega}{h \cdot h'} \leq 2^{1 + \omega - h - h'}.$$

But this last inequality does indeed hold by the Lemma 13.9. □

Bibliography

[Ade] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Math. **1761**, Springer-Verlag, New York, 2001.

[A-W] M. Artin and G. Winters, *Degenerate fibres and stable reduction of curves*, Topology **10** (1971), 373-383.

[Bir] B.J. Birch, *Cyclotomic fields and Kummer extensions.* In Algebraic Number Theory, J.W.S. Cassels and A. Fröhlich eds., Academic Press, London, 1967 85-93.

[B-K] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715-743.

[Coh] H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math. **193**, Springer-Verlag, New York, 2000.

[Cre1] J.E. Cremona, *Algorithms for modular elliptic curves* (2nd Ed.), Cambridge University Press, Cambridge, 1997.

[Cre2] J.E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compos. Math. **51** (1984), 275-324.

[Cre3] J.E. Cremona, Personal e-mail communication, August 19, 2008.

[Cre4] J.E. Cremona, Unpublished tables, http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/iqfdata/

[Edi1] B. Edixhoven, *Minimal resolution and stable reduction*, Ann. Inst. Fourier **40**, 1 (1990), 31-67.

[Edi2] B. Edixhoven, *L'action de l'algèbre de Hecke sur le groupe des composantes des Jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque **196-197** (1991), 159-170.

[Fon] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515-538.

[Kag] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta Arith. **3** (2001), 231-245.

[Kaw] Y. Kawada, *On the ramification theory of infinite algebraic extensions*, Ann. of Math. (2) **58** (1953), 24-47.

[Klu] A. Klute, *Icosahedral Galois extensions and elliptic curves*, Manuscripta Math. **93** (1997), 301-324.

[Lan] S. Lang, *Algebraic number theory*, Grad. Texts in Math. **110**, Springer-Verlag, New York, 1994.

[Liu] Q. Liu, *Algebraic geometry and arithmetic curves*, Translated from French by Reinie Erné, Oxf. Grad. Texts in Math. **6**, Oxford University Press, New York, 2002.

[Lor1] D. Lorenzini, *Arithmetical graphs*, Math. Ann. **285** (1989), 481-501.

[Lor2] D. Lorenzini, *Frobenius number, Riemann-Roch structure, and zeta functions of graphs*, Preprint.

[Lor3] D. Lorenzini, *Groups of components of Néron models of Jacobians*, Compos. Math. **73** (1990), 145-160.

[Lor4] D. Lorenzini, *Reduction of points in the group of components of the Néron model of a jacobian*, J. Reine angew. Math **430** (2000), 117-150.

[Pgp] **PARI/GP**, version 2.3.0, Bordeaux, 2006.

[Pin] R. Pinch, *Elliptic curves with good reduction away from 3*, Math. Proc. Cambridge Philos. Soc. **101** (1987), 451-459.

[Ray] M. Raynaud, *Spécialisation du foncteur de Picard*, Inst. Hautes Études Sci. Publ. Math. **38** (1970), 27-70.

[Rot] J. Rotman, *A first course in abstract algebra* (2nd edition), Prentice Hall, Upper Saddle River, NJ, 2000.

[Ser1] J.-P. Serre, *Local fields*, Translated from French by Marvin J. Greenberg, Grad. Texts in Math. **106**, Springer-Verlag, New York, 1979.

[Ser2] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Set] B. Setzer, *Elliptic curves of prime conductor*, J. of London Math. Soc. (2) **10** (1975), 367-378.

[Shu] R.-M. Shumbusho, *Elliptic curves with prime conductor and a conjecture of Cremona*, Unpublished Ph.D. thesis, University of Georgia, 2004.

[Sil1] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer-Verlag, New York, 1994.

[Sil2] J. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Springer-Verlag, New York, 1986.

[Win] G. Winters, *On the existence of certain families of curves*, Amer. J. of Math.**96** (1974), 215-228 .

Appendix A

Programs for computing the factorization of (3) in $K(\Delta^{\frac{1}{3}})$ and the class number of $K(\Delta^{\frac{1}{3}})$

Let $K = \mathbb{Q}(\sqrt{d})$ where $d = 4k + 1$ with $k \leq -2$. Let p be a prime number. Let (π) be a prime of $\mathcal{O}_K$ be a prime of K lying above (3).

Consider the two field extensions $K(\pi^{\frac{\epsilon}{3}})$ for $\epsilon = 1, 2$. For each we aim to compute the class number of $K(\pi^{\frac{\epsilon}{3}})$ as well as the ramification and inertial indices of the factorization of (3) in $K(\pi^{\frac{\epsilon}{3}})$.

When $(\frac{d}{p}) \neq -1$ (i.e., p is not inert in K) the following **GP/PARI** code performs the two above tasks.

```
d=
p=
K=bnfinit(y^2-y+(1-d)/4);
P=idealprimedec(K,p);
q=P[1];
r=bnfisprincipal(K,q);
a=r[2][1];
b=r[2][2];
g=x^3-Mod(a+b*y,y^2-y+(1-d)/4);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp


g=x^3-Mod((a+b*y)^2,y^2-y+(1-d)/4);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp
```

When $(\frac{d}{p}) = -1$ (i.e., p is inert in K) the following **GP/PARI** code performs the two above tasks.

```
d=
p=
f=polcompositum(x^2-d, x^3-p)[1];
L=bnfinit(f);
idealprimedec(L,3)
L.clgp


ff=polcompositum(x^2-d, x^3-p^2)[1];
LL=bnfinit(ff);
idealprimedec(LL,3)
LL.clgp
```

Now let $K = \mathbb{Q}(\sqrt{d})$ where $d = -1$. Let p be a prime number. Let (π) be a prime of $\mathcal{O}_K$ be a prime of K lying above (3).

Consider the four field extensions $K(\pi^{\frac{\epsilon}{3}})$ and $K(i \cdot \pi^{\frac{\epsilon}{3}})$ for $\epsilon = 1, 2$. For each we aim to compute its class number as well as the ramification and inertial indices of the factorization of (3) in the field itself.

When $(\frac{d}{p}) \neq -1$ (i.e., p is not inert in K) the following **GP/PARI** code performs the two above tasks.

```
d=-1
p=
K=bnfinit(y^2-d);
P=idealprimedec(K,p);
q=P[1];
r=bnfisprincipal(K,q);
a=r[2][1];
b=r[2][2];
g=x^3-Mod(a+b*y,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp
```

```
g=x^3-Mod(-b+a*y,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp


g=x^3-Mod((a+b*y)^2,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp



g=x^3-Mod(-2*a*b+(a^2-b^2)*y,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp
```

When $(\frac{d}{p}) = -1$ (i.e., p is inert in K) the following **GP/PARI** code performs the two above tasks.

```
d=-1
p=
f=polcompositum(x^2-d,x^3-p)[1];
L=bnfinit(f);
idealprimedec(L,3)
L.clgp

ff=polcompositum(x^2-d,x^3-p^2)[1];
LL=bnfinit(ff);
idealprimedec(LL,3)
LL.clgp
```

```
K=bnfinit(y^2-d);
g=x^3-Mod(p*y,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp
```

```
g=x^3-Mod((p^2)*y,y^2-d);
L=rnfinit(K,g);
Leqn=rnfequation(K,g,1)[1];
Labs=bnfinit(Leqn);
idealprimedec(Labs,3)
Labs.clgp
```

Appendix B

Programs for computing the g-integer of an arbitrary arithmetical graph

In this appendix we give the code of a program using the python language and the SAGE interface that computes a host of invariants of any arithmetical graph.

In the main function the user enters the R (here as a row vector) and the matrix M. The program starts by computing and displaying the orders of the cyclic factors of $\Phi(M)$ when decomposed as a product of finite cyclic groups. It also determines and displays the value of $g_0(M)$. It then starts at $d := g_0(M) - 1$ and computes the number of degree d classes represented by an effective divisor. It decreases d by 1 and repeats this until it finds fewer than $\phi(M)$ such classes for d. Once this happens $g(M)$ is found. In the process of doing this repetition any divisor class of degree d that is represented by an effective divisor will have an effective representative for it printed out. It then computes all the degree $2g(M)-2$ effective classes (which are necessarily $\phi(M)$ in number) and then goes down this list one by one and checks which (if any) are canonical divisors. Finally, the g-integer is displayed along with the number of canonical classes and (if any) representatives of these divisor classes.

As written in this appendix the program is set to compute the arithmetical graph associated to the minimal regular model of $X_0(169)$ over $\mathbb{Q}_{13}^{unr}$. The generated output for this example is included below (after the code).

```
def effective_class_number_check(M_temp,list_temp,i_temp,phi_temp):
   listz=[list_temp[0]]
   print listz[0],len(listz)
   i=0
   while len(listz)<phi_temp and i<len(list_temp)-1:
      i=i+1
      check=True
      for j in range(0,len(listz)):
         tempvect=[]
         firsttemp=list_temp[i]
         secondtemp=listz[j]
```

```
         for y in range(0,len(list_temp[0])):
            tempvect=tempvect+[firsttemp[y]-secondtemp[y]]
         ab=gap.SolutionIntMat(M_temp,tempvect)
         cd=gap.IsBool(ab)
         ef=eval(str(cd))
         if ef==False:
            check=False
      if check==True:
         listz=listz+[list_temp[i]]
         print listz[len(listz)-1],len(listz)
   print ""
   print len(listz),"is the number of classes of
   degree",i_temp,"represented by an effective"
   print "-----------------------------------------------
   -------------------"
   return listz


def thing(vectss,i_temp,R_temp):
   vectsss=[]
   finished=False
   j=len(R_temp)-1
   while finished==False and 0<=j:
      if i_temp<R_temp[j]*(vectss[j]+1):
         j=j-1
      else:
         finished=True
   if  j==-1:
      return vectss,False
   else:
      for k in range(len(R_temp)):
           if k==j:
               vectsss=vectsss+[vectss[j]+1]
            elif j<k:
               vectsss=vectsss+[0]
            else:
               vectsss=vectsss+[vectss[k]]
      return vectsss,True


def main():
      R=[12,6,4,1,1]
      M=[[1,-1,-1,-1,-1],[-1,2,0,0,0],[-1,0,3,0,0],[-1,0,0,13,-1],
```

```
[-1,0,0,-1,13]]
number_of_vertices=len(R)
phi=1
linear_rank=0
for i in range(len(R)):
    linear_rank=linear_rank+R[i]*(M[i][i]-2)
linear_rank=(linear_rank+2)/2
invariant_factors=[]
A=gap.SmithNormalFormIntegerMat(M)
for ik in range(1,number_of_vertices):
   if 1<A[ik][ik]:
      invariant_factors+=[A[ik][ik]]
      phi=phi*(A[ik][ik])
if 1<len(invariant_factors):
   print "The component group has order",phi
   print "The component group is of type (",
   for i in range(len(invariant_factors)):
      print invariant_factors[i],
      if i!=len(invariant_factors)-1:
         print ",",
   print ")"
elif len(invariant_factors)==1:
   print "The component group is cyclic of order",invariant_factors[0]
else:
   print "The component group has order 1"
print "The linear rank is",linear_rank
print ""
if linear_rank==0:
   g=0
if linear_rank==1 and phi!=1:
   g=1
if linear_rank==1 and phi==1:
   g=0
if 1<linear_rank:
   totally_done=False
   i=linear_rank
   while totally_done==False and 1!=i:
      i=i-1
      vect=[]
      for u in range(0,len(R)):
         vect=vect+[0]
      final=[]
      done=False
```

```
while (done==False):
   vectssss,decision=thing(vect,i,R)
   vect=vectssss
   if decision==False:
      done=True
   else:
      degree_of_vectz=0
      for z in range(0,len(R)):
         degree_of_vectz=degree_of_vectz+R[z]*vect[z]
      if degree_of_vectz==i:
         final.append(vect)
if 0==len(final):
   totally_done=True
   g=i+1
if 1==len(final) and phi!=1:
   totally_done=True
   g=i+1
if 1==len(final) and phi==1:
   done=True
else:
   list_of_classes=effective_class_number_check(M,final,i,phi)
if len(list_of_classes)<phi:
   totally_done=True
   g=i+1
   vectt=[]
   for uu in range(0,len(R)):
      vectt=vectt+[0]
   finall=[]
   donee=False
   while (donee==False):
      vecttssss,decisionn=thing(vectt,2*g-2,R)
      vectt=vecttssss
      if decisionn==False:
         donee=True
      else:
         degree_of_vectzz=0
         for zz in range(0,len(R)):
            degree_of_vectzz=degree_of_vectzz+R[zz]*vectt[zz]
         if degree_of_vectzz==2*g-2:
            finall=finall+[vectt]
   list_of_classess=
   effective_class_number_check(M,finall,2*g-2,phi)
   canonical_list=[]
```

```
                for q in range(0,len(list_of_classess)):
                   t=-1
                   check3=True
                   while (check3==True and t<=len(list_of_classes)-2):
                      t=t+1
                      i=-1
                      check2=False
                      while (check2==False and i<=len(list_of_classes)-2):
                         i=i+1
                         ttt=[]
                         for cc in range(0,len(R)):
                            aaa=list_of_classess[q]
                            bbb=list_of_classes[t]
                            ddd=list_of_classes[i]
                            ttt=ttt+[aaa[cc]-bbb[cc]-ddd[cc]]
                         uuu=gap.SolutionIntMat(M,ttt)
                         vvv=gap.IsBool(uuu)
                         www=eval(str(vvv))
                         if www==False:
                            check2=True
                      if check2==False:
                         check3=False
                   if check3==True:
                      canonical_list=canonical_list+[list_of_classess[q]]
      if i==1 and g!=2:
         if phi==1:
            g=0
         else:
            g=1
      print "The g-integer is",g
      print "The number of canonical classes is",len(canonical_list)
      print "These classes are",canonical_list
      print ""
      print ""
main()
```

Once the above program runs on $X_0(169)/\mathbb{Q}_{13}^{unr}$ (see Chapter 13) it outputs:

```
The component group is cyclic of order 7
The linear rank is 8

[0, 0, 0, 0, 7] 1
```

```
[0, 0, 0, 1, 6] 2
[0, 0, 0, 2, 5] 3
[0, 0, 0, 3, 4] 4
[0, 0, 0, 4, 3] 5
[0, 0, 0, 5, 2] 6
[0, 0, 0, 6, 1] 7

7 is the number of classes of degree 7 represented by an effective
------------------------------------------------------------------
[0, 0, 0, 0, 6] 1
[0, 0, 0, 1, 5] 2
[0, 0, 0, 2, 4] 3
[0, 0, 0, 3, 3] 4
[0, 0, 0, 4, 2] 5
[0, 0, 0, 5, 1] 6
[0, 0, 0, 6, 0] 7

7 is the number of classes of degree 6 represented by an effective
------------------------------------------------------------------
[0, 0, 0, 0, 5] 1
[0, 0, 0, 1, 4] 2
[0, 0, 0, 2, 3] 3
[0, 0, 0, 3, 2] 4
[0, 0, 0, 4, 1] 5
[0, 0, 0, 5, 0] 6

6 is the number of classes of degree 5 represented by an effective
------------------------------------------------------------------
[0, 0, 0, 0, 10] 1
[0, 0, 0, 1, 9] 2
[0, 0, 0, 2, 8] 3
[0, 0, 0, 3, 7] 4
[0, 0, 0, 4, 6] 5
[0, 0, 0, 5, 5] 6
[0, 0, 0, 6, 4] 7

7 is the number of classes of degree 10 represented by an effective
-------------------------------------------------------------------
The g-integer is 6
The number of canonical classes is 1
These classes are [[0, 0, 0, 5, 5]]
```

Appendix C

A program for computing the g-integer of an arithmetical tree with exactly one node

In this appendix we give the code of a program using the python language and the SAGE interface that computes a host of invariants of an arithmetical tree when there is only one node.

Inside the main function the user sets the value for the multiplicity of the node and then the multiplicities (in any order) of the vertices adjacent to the node (the user should personally make sure that the multiplicity of the node divides the sum of the multiplicities of the adjacent vertices or else the result will not be an arithmetical graph). From there the program creates the terminal chains by using Euclid's algorithm (see Remark 4.2 in [Lor1]).

The program starts by computing and outputting R (as a row vector) and M. It then determines and displays the orders of the cyclic factors of $\Phi(M)$ when decomposed as a product of finite cyclic groups. It also determines and displays the value of $g_0(M)$. It then (as in Appendix B) starts at $d := g_0(M) - 1$ and computes the number of degree d classes represented by an effective divisor. It decreases d by 1 and repeats this until it finds fewer than $\phi(M)$ such classes for d. Once this happens $g(M)$ is found. In the process of doing this repetition any divisor class of degree d that is represented by an effective divisor will have an effective representative for it printed out. It then computes all the degree $2g(M)-2$ effective classes (which are necessarily $\phi(M)$ in number) and then goes down this list one by one and checks which (if any) are canonical divisors. Finally, the g-integer is displayed along with the number of canonical classes and (if any) representatives of these divisor classes.

As written in this appendix the program is set to compute Example 11.1. The generated output is included below (after the code).

```
def effective_class_number_check(M_temp,list_temp,i_temp,phi_temp):
   listz=[list_temp[0]]
   print listz[0],len(listz)
   i=0
```

```
   while len(listz)<phi_temp and i<len(list_temp)-1:
      i=i+1
      check=True
      for j in range(0,len(listz)):
         tempvect=[]
         firsttemp=list_temp[i]
         secondtemp=listz[j]
         for y in range(0,len(list_temp[0])):
            tempvect=tempvect+[firsttemp[y]-secondtemp[y]]
         ab=gap.SolutionIntMat(M_temp,tempvect)
         cd=gap.IsBool(ab)
         ef=eval(str(cd))
         if ef==False:
            check=False
      if check==True:
         listz=listz+[list_temp[i]]
         print listz[len(listz)-1],len(listz)
   print ""
   print len(listz),"is the number of classes of
   degree",i_temp,"represented by an effective"
   print "-------------------------------------------------
   -----------------"
   return listz


def thing(vectss,i_temp,R_temp,terminal_temp):
   vectsss=[]
   finished=False
   j=len(terminal_temp)-1
   while finished==False and 0<=j:
      if i_temp<R_temp[terminal_temp[j]]*(vectss[terminal_temp[j]]+1):
         j=j-1
      else:
         finished=True
   if  j==-1:
      return vectss,False
   else:
      for k in range(len(R_temp)):
         if k in terminal_temp:
            if k==terminal_temp[j]:
               vectsss=vectsss+[vectss[terminal_temp[j]]+1]
            elif terminal_temp[j]<k:
               vectsss=vectsss+[0]
```

```
            else:
               vectsss=vectsss+[vectss[k]]
         else:
            vectsss=vectsss+[0]
      return vectsss,True


def main():
      node_mult=8
      S=[3,2,1,1]
      R=[node_mult]
      number_of_chains=len(S)
      chain_lengths=[]
      sum_S=0
      for i in range(number_of_chains):
         sum_S+=S[i]
     chain_length_count=1
     R=R+[S[i]]
 temp=S[i]
 if node_mult%temp==0:
            chain_lenghts=chain_lengths+[1]
     else:
           tempa=-((node_mult%temp)-temp)
           R=R+[tempa]
           checker=False
           chain_length_count=1
           while checker==False:
               if temp%tempa==0:
                  chain_length_count=chain_length_count+1
                  checker=True
               else:
                  tempb=-((temp%tempa)-tempa)
                  temp=tempa
                  tempa=tempb
                  R=R+[tempb]
                  chain_length_count=chain_length_count+1
         chain_lengths=chain_lengths+[chain_length_count]
      print "R=",R
      number_of_vertices=1
      node_adjacent_indices=[1]
      for i in range(1,len(S)):
         number_of_vertices+=chain_lengths[i-1]
         node_adjacent_indices+=[number_of_vertices]
```

```
number_of_vertices+=chain_lengths[len(S)-1]
M=[]
for i in range(number_of_vertices):
   zero_vector=[]
   for j in range(number_of_vertices):
      zero_vector+=[0]
   M+=[zero_vector]
M[0][0]=sum_S/R[0]
for i in range(len(S)-1):
   M[0][node_adjacent_indices[i]]=-1
   for j in range(node_adjacent_indices[i]+1,
   node_adjacent_indices[i+1]):
      M[0][j]=0
M[0][node_adjacent_indices[len(S)-1]]=-1
if node_adjacent_indices[len(S)-1]+1<=number_of_vertices-1:
   for i in range(node_adjacent_indices[len(S)-1]+1,
   number_of_vertices):
      M[0][i]=0
tempholder=node_adjacent_indices+[number_of_vertices]
for i in range(len(S)):
   for j in range(tempholder[i],tempholder[i+1]):
      for k in range(number_of_vertices):
         if j==k and j==tempholder[i] and j!=tempholder[i+1]-1:
            M[j][k]=(R[0]+R[j+1])/R[j]
         elif j==k and j!=tempholder[i] and j==tempholder[i+1]-1:
            M[j][k]=R[j-1]/R[j]
         elif j==k and j==tempholder[i] and j==tempholder[i+1]-1:
            M[j][k]=R[0]/R[j]
         elif j==k and j!=tempholder[i] and j!=tempholder[i+1]-1:
            M[j][k]=(R[j-1]+R[j+1])/R[j]
         elif k==0 and j==tempholder[i]:
            M[j][k]=-1
         elif (2<=k-j or 2<=j-k) and k!=0:
         M[j][k]=0
 elif k-j==1 and j!=tempholder[i+1]-1:
     M[j][k]=-1
 elif j-k==1 and j!=tempholder[i]:
     M[j][k]=-1
number_of_vertices=len(R)
print "M is the following matrix:"
for i in range(number_of_vertices):
   print M[i]
linear_rank=R[0]*(len(S)-2)-R[number_of_vertices-1]
```

```
terminal_indices=[]
for i in range(1,len(S)):
   terminal_indices+=[tempholder[i]-1]
   linear_rank-=R[tempholder[i]-1]
terminal_indices+=[number_of_vertices-1]
linear_rank=linear_rank/2+1
phi=1
invariant_factors=[]
A=gap.SmithNormalFormIntegerMat(M)
for ik in range(1,number_of_vertices):
   if 1<A[ik][ik]:
      invariant_factors+=[A[ik][ik]]
      phi=phi*(A[ik][ik])
if 1<len(invariant_factors):
   print "The component group has order",phi
   print "The component group is of type (",
   for i in range(len(invariant_factors)):
      print invariant_factors[i],
      if i!=len(invariant_factors)-1:
         print ",",
   print ")"
elif len(invariant_factors)==1:
   print "The component group is cyclic of order",invariant_factors[0]
else:
   print "The component group has order 1"
print "The linear rank is",linear_rank
if linear_rank==0:
   g=0
if linear_rank==1 and phi!=1:
   g=1
if linear_rank==1 and phi==1:
   g=0
if 1<linear_rank:
   totally_done=False
   i=linear_rank
   while totally_done==False and 1!=i:
      i=i-1
      vect=[]
      for u in range(0,len(R)):
         vect=vect+[0]
      final=[]
      done=False
      while (done==False):
```

```
   vectssss,decision=thing(vect,i,R,terminal_indices)
   vect=vectssss
   if decision==False:
      done=True
   else:
      degree_of_vectz=0
      for z in range(0,len(R)):
         degree_of_vectz=degree_of_vectz+R[z]*vect[z]
      if degree_of_vectz==i:
         final.append(vect)
if 0==len(final):
   totally_done=True
   g=i+1
if 1==len(final) and phi!=1:
   totally_done=True
   g=i+1
if 1==len(final) and phi==1:
   done=True
else:
   list_of_classes=effective_class_number_check(M,final,i,phi)
if len(list_of_classes)<phi:
   totally_done=True
   g=i+1
   vectt=[]
   for uu in range(0,len(R)):
      vectt=vectt+[0]
   finall=[]
   donee=False
   while (donee==False):
      vecttssss,decisionn=thing(vectt,2*g-2,R,terminal_indices)
      vectt=vecttssss
      if decisionn==False:
         donee=True
      else:
         degree_of_vectzz=0
         for zz in range(0,len(R)):
            degree_of_vectzz=degree_of_vectzz+R[zz]*vectt[zz]
         if degree_of_vectzz==2*g-2:
            finall=finall+[vectt]
   list_of_classess=effective_class_number_check(M,
   finall,2*g-2,phi)
   canonical_list=[]
   for q in range(0,len(list_of_classess)):
```

```
                t=-1
                check3=True
                while (check3==True and t<=len(list_of_classes)-2):
                   t=t+1
                   i=-1
                   check2=False
                   while (check2==False and i<=len(list_of_classes)-2):
                      i=i+1
                      ttt=[]
                      for cc in range(0,len(R)):
                         aaa=list_of_classess[q]
                         bbb=list_of_classes[t]
                         ddd=list_of_classes[i]
                         ttt=ttt+[aaa[cc]-bbb[cc]-ddd[cc]]
                      uuu=gap.SolutionIntMat(M,ttt)
                      vvv=gap.IsBool(uuu)
                      www=eval(str(vvv))
                      if www==False:
                         check2=True
                   if check2==False:
                      check3=False
                if check3==True:
                   canonical_list=canonical_list+[list_of_classess[q]]
      if i==1:
         if phi==1:
            g=0
         else:
            g=1
      print "The g-integer is",g
      print "The number of canonical classes is",len(canonical_list)
      print "These classes are",canonical_list
      print ""
      print ""
main()
```

Once the above program runs on Example 11.1 it outputs:

```
R= [8, 3, 1, 2, 2, 1]
M is the following matrix:
[1, -1, 0, -1, -1, -1]
[-1, 3, -1, 0, 0, 0]
[0, -1, 3, 0, 0, 0]
```

```
[-1, 0, 0, 4, 0, 0]
[-1, 0, 0, 0, 4, 0]
[-1, 0, 0, 0, 0, 8]
The component group has order 16
The component group is of type ( 4 , 4 )
The linear rank is 6

[0, 0, 0, 0, 0, 5] 1
[0, 0, 0, 0, 1, 3] 2
[0, 0, 0, 0, 2, 1] 3
[0, 0, 0, 1, 0, 3] 4
[0, 0, 0, 1, 1, 1] 5
[0, 0, 0, 2, 0, 1] 6
[0, 0, 1, 0, 1, 2] 7
[0, 0, 1, 0, 2, 0] 8
[0, 0, 1, 1, 0, 2] 9
[0, 0, 1, 1, 1, 0] 10
[0, 0, 1, 2, 0, 0] 11
[0, 0, 2, 0, 1, 1] 12
[0, 0, 2, 1, 0, 1] 13
[0, 0, 3, 0, 0, 2] 14
[0, 0, 3, 0, 1, 0] 15
[0, 0, 3, 1, 0, 0] 16

16 is the number of classes of degree 5 represented by an effective
------------------------------------------------------------------
[0, 0, 0, 0, 0, 4] 1
[0, 0, 0, 0, 1, 2] 2
[0, 0, 0, 0, 2, 0] 3
[0, 0, 0, 1, 0, 2] 4
[0, 0, 0, 1, 1, 0] 5
[0, 0, 0, 2, 0, 0] 6
[0, 0, 1, 0, 1, 1] 7
[0, 0, 1, 1, 0, 1] 8
[0, 0, 2, 0, 0, 2] 9
[0, 0, 2, 0, 1, 0] 10
[0, 0, 2, 1, 0, 0] 11
[0, 0, 3, 0, 0, 1] 12

12 is the number of classes of degree 4 represented by an effective
------------------------------------------------------------------
[0, 0, 0, 0, 0, 8] 1
[0, 0, 0, 0, 1, 6] 2
```

```
[0, 0, 0, 0, 2, 4] 3
[0, 0, 0, 0, 3, 2] 4
[0, 0, 0, 1, 0, 6] 5
[0, 0, 0, 1, 1, 4] 6
[0, 0, 0, 1, 2, 2] 7
[0, 0, 0, 1, 3, 0] 8
[0, 0, 0, 2, 0, 4] 9
[0, 0, 0, 2, 1, 2] 10
[0, 0, 0, 2, 2, 0] 11
[0, 0, 0, 3, 0, 2] 12
[0, 0, 0, 3, 1, 0] 13
[0, 0, 1, 1, 2, 1] 14
[0, 0, 1, 2, 1, 1] 15
[0, 0, 2, 1, 1, 2] 16

16 is the number of classes of degree 8 represented by an effective
------------------------------------------------------------------
The g-integer is 5
The number of canonical classes is 0
These classes are []
```