ARITHMETIC INTERSECTIONS ON NON-SPLIT CARTAN MODULAR CURVES

JONATHAN LOVE, ÉLIE STUDNIA, AND JAN VONK

Abstract. Let p be a prime number, and let $\Delta_1, \Delta_2 < 0$ be two coprime fundamental discriminants. When p *splits* in $\mathbb{Q}(\sqrt{\Delta_1})$ and $\mathbb{Q}(\sqrt{\Delta_2})$ the height pairings of the corresponding CM divisors on $X_{\mathrm{sp}}^+(p)$ were determined by Gross–Kohnen–Zagier [GKZ87]. When p is *inert*, we determine the arithmetic intersection numbers of the corresponding divisors on $X_{\mathrm{ns}}^+(p)$ at all finite primes. The key point of our analysis is at the prime of bad reduction p: to determine the intersection numbers at p, we provide a moduli interpretation for the smooth locus in the regular model of $X_{\mathrm{ns}}^+(p)$ over $\mathrm{Spec}(\mathbb{Z})$ constructed by Edixhoven–Parent [EP24].

Contents

1. Introduction

The work of Heegner [Hee52] reduces the classification of negative discriminants of class number one to the determination of integer solutions to the Diophantine equation

$$y^2 = x^3 + 8. \tag{1}$$

As explained by Serre [Ser97, Appendix], the strategy of Heegner may be interpreted, and framed more generally, as the determination of the set of rational points, integral with respect to the cusps, on a non-split Cartan modular curve $X_{\mathrm{ns}}^+(N)$. The case employed by Heegner is $X_{\mathrm{ns}}^+(24)$ which is an elliptic curve described by the equation (1). Siegel [Sie68] similarly considered the elliptic curve $X_{\mathrm{ns}}^+(15)$, and used it to give an alternative proof[1] of the class number one problem.

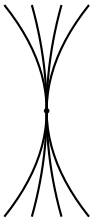
In spite of this momentous early application of CM points on non-split Cartan curves, our knowledge on rational points on $X_{\mathrm{ns}}^+(p)$ remains limited. It is the sole remaining obstacle for establishing Serre uniformity [Ser72], which asks whether there exists a constant C such that the Galois representation

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

[1]The first proof with prime level was given by Kenku [Ken85] for $N = 7$. The curve $X_{\mathrm{ns}}^+(11)$ is an elliptic curve of rank one, see Ligozat [Lig77], and has also been used to resolve the class number one problem by Schoof–Tzanakis [ST12]. The rational points on $X_{\mathrm{ns}}^+(13)$ and $X_{\mathrm{ns}}^+(17)$, curves of genus 3 and 6 respectively, have also been determined [BDMTV19; BDMTV23].

is surjective for all non-CM elliptic curves $E/\mathbb{Q}$, and all primes $p > C$. It is widely believed that $C = 37$ suffices. The work of Serre [Ser72], Mazur [Maz77], Bilu–Parent–Rebolledo [BP11; BPR13] reduces this to the question of whether $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ consists entirely of CM points, for p large enough.

This paper makes a study of the arithmetic geometry of non-split Cartan modular curves, and their CM points. Our first result concerns a moduli interpretation over $\mathrm{Spec}(\mathbb{Z})$ of the minimal regular model.



Edixhoven–Parent [EP24] determine a minimal regular model for $X_{\mathrm{ns}}^+(p)$ over $W(\overline{\mathbb{F}}_p)$. It is constructed from the models of Katz–Mazur [KM85] for $X(p)$ via a sequence of blow-ups, quotients, and blow-downs. Its special fibre at p consists of a collection of projective lines, indexed by the supersingular j-invariants, which all meet at one point. They remark:

> *"Those $\mathbb{P}^1$s [...] in the non-split cases have no modular interpretation, as they just result from blow-ups in the course of the regularization process."*

Section 2 offers a moduli interpretation for the smooth locus of this model. It relies on the observation that an elliptic curve with non-split Cartan structure defined over $\mathbb{Q}_p^{\mathrm{ur}}$ has supersingular reduction if $p > 7$. More generally, for any prime p and $n \geq 1$, we study the coarse moduli space over $\mathrm{Spec}(\mathbb{Z})$ of the functor

$$\begin{array}{rccl} \mathcal{M}_{\mathrm{ns}}^+(p^n): & \underline{\mathbf{Sch}}_{\mathbb{Z}} & \longrightarrow & \underline{\mathbf{Set}} \\ & S & \longmapsto & \{E/S \text{ with } \mathbb{Z}_{p^2}/(p^n) \hookrightarrow \mathrm{End}_S(E[p^n])\}/\sim \end{array} \tag{2}$$

of isomorphism classes of elliptic curves E/S with an embedding of $\mathbb{Z}_{p^2}/(p^n)$ into the endomorphism ring of the group scheme $E[p^n]$ over S, with conjugate embeddings identified. Here, $\mathbb{Z}_{p^2}$ is the Witt ring of $\mathbb{F}_{p^2}$.

The special fibre is a disjoint union of $\mathbb{A}^1$'s, which may be explained as follows. For a supersingular elliptic curve $E/S/\mathbb{F}_p$, $E[p]$ represents a non-trivial class in $\mathrm{Ext}_S^1(\boldsymbol{\alpha}_p, \boldsymbol{\alpha}_p)$. Given an element λ of $\mathrm{End}_S(\boldsymbol{\alpha}_p/S) \simeq \mathbb{A}^1(S)$ we obtain an endomorphism of $E[p^n]$ by composition

$$E[p^n] \xrightarrow{p^{n-1}} E[p] \longrightarrow \boldsymbol{\alpha}_p \xrightarrow{\lambda} \boldsymbol{\alpha}_p \longrightarrow E[p] \longrightarrow E[p^n]. \tag{3}$$

This induces an action of $\mathbb{A}^1(S)$ on the set $\{\mathbb{Z}_{p^2}/(p^n) \hookrightarrow \mathrm{End}_S(E[p^n])\}$ by adding this endomorphism to the image of a fixed algebra generator of $\mathbb{Z}_{p^2}/(p^n)$. The first main result is:

Theorem A. *Let p be a prime number. The coarse moduli scheme $\mathscr{X}_{\mathrm{ns}}^+(p^n)$ associated with (2) is smooth over $\mathrm{Spec}(\mathbb{Z})$. Its geometric special fibre at p is the disjoint union of finitely many[2] components isomorphic to $\mathbb{A}^1$.*

When $n = 1$ the set of components in the special fibre are canonically in bijection with the isomorphism classes of supersingular elliptic curves E over $\overline{\mathbb{F}}_p$. In § 2.5 we show that $\mathscr{X}_{\mathrm{ns}}^+(p)$ is isomorphic to the smooth non-cuspidal locus of the minimal regular model constructed by Edixhoven–Parent for $p > 7$.

The second result of this paper is an explicit determination of the arithmetic intersection of a pair of Heegner points on $\mathscr{X}_{\mathrm{ns}}^+(p^n)$, similar to the result of Gross–Kohnen–Zagier [GKZ87]. Let $\Delta_1, \Delta_2 < 0$ be a pair of coprime fundamental discriminants such that p is *inert* in both $K_1 := \mathbb{Q}(\sqrt{\Delta_1})$ and $K_2 := \mathbb{Q}(\sqrt{\Delta_2})$. There are two associated Heegner divisors, of degrees equal to the class numbers of K_1 and K_2:

$$P_1, P_2 \in \mathrm{Div}_{\mathbb{Q}}(X_{\mathrm{ns}}^+(p^n)).$$

Their Zariski closures in the integral model $\mathscr{X}_{\mathrm{ns}}^+(p^n)$ over $\mathbb{Z}$ constructed in theorem A intersect properly, and we explicitly determine their arithmetic intersection number

$$\langle P_1, P_2 \rangle := \sum_{x \in \mathrm{Max}\, \mathscr{X}_{\mathrm{ns}}^+(p^n)} \mathrm{length}\left(\frac{\mathcal{O}_{\mathscr{X},x}}{(P_1, P_2)}\right) \cdot \log|k_x| \tag{4}$$

[2] When $p \geq 5$, the number of components is the sum of $1 + \frac{2(p^{2n-2}-1)}{|\mathrm{Aut}(E)|}$ over all supersingular curves $E/\overline{\mathbb{F}}_p$, see remark 2.22.

where x ranges over closed points on $\mathscr{X}^+_{\mathrm{ns}}(p^n)$, and we denote k_x for its residue field. Using theorem A, we reduce the problem to counting, for each prime q, embeddings of quadratic orders

$$\mathcal{O}_1, \mathcal{O}_2 \;\hookrightarrow\; R \subset B_{q\infty}, \qquad \mathrm{disc}(\mathcal{O}_i) = \Delta_i.$$

Instead of the Eichler orders arising in [GKZ87], we are faced with *non-split Cartan orders* R (definition 3.5). These orders are not Eichler, but they are Bass (or basic) orders in the sense of [CSV21]. To state the explicit formula for the intersection number $\langle P_1, P_2\rangle$, we define for any positive integers $a, b \in \mathbb{Z}$ the finite set

$$\mathcal{S}(a,b) := \mathbb{Z}_{>0} \,\cap\, \left\{ \frac{a - x^2}{4b} : x \in \mathbb{Z} \right\}. \tag{5}$$

We define the map ϵ as in Gross–Zagier [GZ85, p. 192]: Let $F = \mathbb{Q}(\sqrt{\Delta_1\Delta_2})$ and χ the genus character of F associated to K_1K_2/F. For any prime q define $\epsilon(q) := \chi(\mathfrak{q})$ where $\mathfrak{q}$ is any prime in F above q. Extend the definition of ϵ multiplicatively. The following result is proved in § 3:

Theorem B. *The intersection number of P_1 and P_2 on the arithmetic surface $\mathscr{X}^+_{\mathrm{ns}}(p^n)$ is given by*

$$\langle P_1, P_2\rangle \;=\; \frac{w_1 w_2}{4} \cdot \sum_{\substack{m \in \mathcal{S}(\Delta_1\Delta_2,\, p^{2n}) \\ d \,|\, m,\; d>0}} \epsilon\left(\frac{m}{d}\right) \log(d), \qquad \textit{where } \; w_i := |\,\mathcal{O}_i^\times\,|. \tag{6}$$

When p *splits* in the quadratic fields K_1 and K_2 the arguments of Gross–Kohnen–Zagier [GKZ87] show that the intersection numbers of the Heegner divisors on the *split* Cartan normaliser curve $X^+_{\mathrm{sp}}(p^n)$ are given by the same formula. A notable difference is that in the split case, the CM elliptic curves have *ordinary* reduction at p, and thus cannot intersect in the bad fibre. In the inert case however, the elliptic curves are *supersingular* at p and therefore may (and frequently do) intersect in the bad fibre.

Example 1.1. Consider $X^+_{\mathrm{ns}}(11)$, which is an elliptic curve with minimal Weierstraß model

$$X^+_{\mathrm{ns}}(11) : y^2 + y = x^3 - x^2 - 7x + 10. \tag{7}$$

The minimal regular model at 11 has Kodaira type III, with one component for each of the two supersingular j-invariants. The Heegner discriminants $(\Delta_1, \Delta_2) = (-115, -267)$ give rise to points

$$P_1 = \left(\sqrt{5},\, \frac{-5+\sqrt{5}}{2}\right), \qquad P_2 = \left(\frac{33+\sqrt{89}}{25},\, \frac{189 - 17\sqrt{89}}{250}\right),$$

which have a simple intersection at 11 on the $j = 1$ component. There is another simple intersection at the prime 5. This is precisely as predicted by theorem B, since $\mathcal{S}(\Delta_1\Delta_2, 11^2) = \{20, 44\}$ and the sum on the right hand side of (6) evaluates to

$$\log\left(\frac{2\cdot 5\cdot 20}{4\cdot 10}\right) + \log\left(\frac{2\cdot 11\cdot 44}{4\cdot 22}\right) = \log(55).$$

In the body of this paper, a more general version of theorem B is proved for modular curves with split Cartan level at some primes, and non-split Cartan level at other primes; this is theorem C. Let N_{sp} and N_{ns} be coprime positive integers, and consider $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of the form $\Gamma := \Gamma^+_{\mathrm{sp}}(N_{\mathrm{sp}}) \cap \Gamma^+_{\mathrm{ns}}(N_{\mathrm{ns}})$, see § 2.4. A modular curve associated to such a level structure will be called *mixed Cartan* and denoted

$$X^+_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}}). \tag{8}$$

We will use the phrase *Heegner discriminant for* Γ for any discriminant $\Delta < 0$ that satisfies

$$\left(\frac{\Delta}{q}\right) = 1 \;\text{ for all }\; q \,|\, N_{\mathrm{sp}}, \qquad \text{and} \qquad \left(\frac{\Delta}{q}\right) = -1 \;\text{ for all }\; q \,|\, N_{\mathrm{ns}}. \tag{9}$$

The reader should not confuse this with common usage of "Heegner hypothesis" to mean that all primes dividing the level are split. Note that Heegner [Hee52] was working with primes that are inert, and our terminology is also used in other works on non-split Cartan curves, for instance Kohen–Pacetti [KP16].

Section 4 complements the work of Rebolledo–Wuthrich [RW25]: we determine all arithmetic intersections of any pair of CM points in $X_{\mathrm{ns}}^{+}(p)(\mathbb{Q})$, for any prime p. Table 1 contains a complete list of non-trivial arithmetic intersections, proving the expectation of [RW25] about the completeness of their data.

Finally, we mention that our main results might be of interest for the study of rational points on $X_{\mathrm{ns}}^{+}(p)$ using the geometric quadratic Chabauty method of Edixhoven–Lido [EL23]. The application of the determination of intersection numbers of Heegner points in this context was brought to our attention by Parent, and we refer to the forthcoming paper [HKLLMP] for more details on this topic.

Acknowledgements. We would like to thank Bas Edixhoven and Henri Darmon for several inspiring conversations on the themes of this paper over the years. All three authors were supported by ERC Starting Grant 101076941 ('GAGARIN'). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

2. The moduli space $\mathscr{X}_{\mathrm{ns}}^{+}(p^n)$ over $\mathrm{Spec}(\mathbb{Z})$

The main purpose of this section is to prove theorem A. We do this in greater generality and allow for an extra level structure, assumed to be finite étale at p. Our discussion freely uses the formalism of moduli problems developed in Chapter 4 of [KM85]. Henceforth, we fix a prime p and an integer $n \geq 1$.

We introduce the moduli problems attached to non-split Cartan structures, and study the geometry of their coarse moduli spaces. In characteristic p, only supersingular elliptic curves appear in this moduli space. We begin by describing the p^n-torsion of supersingular elliptic curves, and their endomorphism rings.

2.1. The p^n-torsion of a supersingular elliptic curve.

We first recall some properties of the p^n-torsion schemes of supersingular elliptic curves in characteristic p. In this subsection, fix an elliptic curve E over a perfect field k of characteristic p. Recall that we have an exact sequence

$$0 \to \boldsymbol{\alpha}_p \xrightarrow{\iota} E[p] \xrightarrow{\pi} \boldsymbol{\alpha}_p \to 0, \tag{10}$$

where the closed subgroup $\boldsymbol{\alpha}_p$ is the kernel of the Frobenius isogeny $E \longrightarrow E^{(p)}$.

Lemma 2.1. *For any k-algebra R, we have:*

- *any endomorphism of $E[p]$ over R restricts through ι to an endomorphism of $\boldsymbol{\alpha}_p$ over R,*
- *the following natural maps on Lie algebras are isomorphisms of free R-modules of rank one:*

$$\mathrm{Lie}(\boldsymbol{\alpha}_p/R) \xrightarrow{\iota} \mathrm{Lie}(E[p]/R) \longrightarrow \mathrm{Lie}(E[p^n]/R) \longrightarrow \mathrm{Lie}(E/R),$$

- *there is an isomorphism of $\mathbb{F}_p$-algebras given by the natural map*

$$\mathrm{End}_R(\boldsymbol{\alpha}_p/R) \xrightarrow{\sim} \mathrm{End}(\mathrm{Lie}(\boldsymbol{\alpha}_p/R)) \cong R.$$

Proof. The kernel G of the Frobenius isogeny is a k-group scheme of degree p by e.g. [KM85, (12.2.1)]. Since $E[p]$ is Cartier-dual to itself and $E[p](\bar{k}) = \{0\}$, G is not étale nor Cartier-dual to a finite étale k-group scheme. Therefore, by the Oort–Tate classification, $G \simeq \boldsymbol{\alpha}_p$.

Since ι is also the kernel of Frobenius on $E[p]$, endomorphisms of $E[p]_R$ can be restricted along ι by [SGA3I, Exp. $\mathrm{VII_A}$, 4.1.3]. By [LLR04, Prop. 1.1 (a)], the given maps of Lie algebras are injective and it is enough to show that Frobenius kills $\mathrm{Lie}(E/R)$: this is contained in [SGA3I, Exp. $\mathrm{VII_A}$, 4.1.2].

The Frobenius $\mathbb{A}^1_k \to \mathbb{A}^1_k$ is a morphism of ring schemes, so its kernel $\boldsymbol{\alpha}_p$ is a module over the ring scheme $\mathbb{A}^1_k$. It is not difficult to check that for any k-algebra R, the composition

$$R = \mathbb{A}^1_k(R) \longrightarrow \mathrm{End}(\boldsymbol{\alpha}_p/R) \longrightarrow \mathrm{End}(\mathrm{Lie}(\boldsymbol{\alpha}_p/R)) = R$$

is the identity. It remains to show that the second map is injective. Let $u \in \mathrm{End}(\boldsymbol{\alpha}_p/R)$ act trivially on $\mathrm{Lie}(\boldsymbol{\alpha}_p/R)$. Then u corresponds to an element f of $t^2R[t]/(t^p)$ such that $f(x+y) = f(x) + f(y)$. Expanding $f(t) = \sum_{j=2}^{p-1} c_j t^j$ with $c_j \in R$ shows that $f = 0$, i.e. that $u = 0$. □

Our geometric study of non-split Cartan moduli problems relies on a study of the endomorphism rings of the group scheme $E[p^n]$. It is a classical result, see e.g. [Stu25, Lemma 4.1.4], that the functors

$$\underline{\mathrm{End}}_k(E[p^n]) \ : \ T \longmapsto \mathrm{End}_T(E[p^n]_T) \qquad\qquad \underline{\mathrm{Aut}}_k(E[p^n]) \ : \ T \longmapsto \mathrm{Aut}_T(E[p^n]_T) \tag{11}$$

from k-schemes to sets are representable by an affine ring scheme E_n (resp. group scheme $E_n^\times$) of finite type over k. Likewise, the functor $E_0 = \underline{\mathrm{End}}_k(\boldsymbol{\alpha}_p)$ of group scheme endomorphisms of $\boldsymbol{\alpha}_p$ is a ring scheme. By lemma 2.1, the Lie algebra action yields a canonical isomorphism $E_0 \simeq \mathbb{A}^1_k$ of ring schemes.

Proposition 2.2. *The scheme E_n is smooth of relative dimension 1 over k. The morphism of group schemes*

$$\nu : E_0 = \underline{\mathrm{End}}_k(\boldsymbol{\alpha}_p) \ \longrightarrow \ E_n = \underline{\mathrm{End}}_k(E[p^n])$$

induced by the sequence (3) is an open immersion onto the unit component of E_n.

Proof. Since the maps π and ι from (10) are faithfully flat, resp. a closed immersion, ν is a monomorphism of k-group schemes. Therefore, E_n is equidimensional of positive dimension by [SGA3I, Exp. $\mathrm{VI_B}$, 1.5].

Let R be a k-algebra. Any $u \in \mathrm{End}_R(E[p^n]_R)$ induces an R-linear endomorphism $u^\sharp$ of the finite free R-module $\mathcal{O}(E[p^n]) \otimes_k R$. The rule $u \mapsto \det(u^\sharp) \in R$ defines a morphism of schemes

$$\det : E_n \ \longrightarrow \ \mathbb{A}^1.$$

Since u is an isomorphism iff $u^\sharp$ is an isomorphism of R-modules, one has $E_n^\times = \det^{-1}(\mathbb{A}^1 \backslash \{0\})$, so $E_n^\times \to E_n$ is an open immersion. By [SGA3I, Exp. $\mathrm{VI_B}$, 1.3, 1.5] and [Stu25, Cor. 4.9.3], E_n is smooth of relative dimension 1 and ν is an open immersion. By [SGA3I, Exp. $\mathrm{VI_B}$, 1.4.2], since E_0 is connected, $E_0 \to E_n$ is a closed open immersion onto the unit component of E_n. □

We now determine the ring of connected components of the endomorphism scheme E_n. A *complete* supersingular elliptic curve is a supersingular E/k such that every geometric endomorphism of E is defined over k. Given such an E/k, let $\mathrm{O}_E := \mathrm{End}(E)$ with maximal two-sided ideal $\mathfrak{P}_E \subset \mathrm{O}_E$, and set

$$R_n(E) := \mathrm{O}_E \, / p^{n-1}\mathfrak{P}_E. \tag{12}$$

Proposition 2.3. *Suppose E/k is complete. Then the quotient E_n/E_0 is a finite constant k-scheme, and the obvious map $\mathrm{O}_E \to E_n(k)$ induces an isomorphism*

$$R_n(E) \simeq (E_n/E_0)(k).$$

Proof. By [SGA3I, Exp. $\mathrm{VI_A}$, 5.5], the quotient $Q := E_n/E_0$ exists and is étale over k. Since $E_n \to Q$ is surjective, Q is quasi-compact hence finite étale. The claim holds over $\overline{k}$ by a Dieudonné module calculation (in the proof of [Stu25, Prop 4.9.4], replace automorphisms with endomorphisms). Because $\mathrm{End}(E) = \mathrm{End}(E_{\overline{k}})$, one has $Q(k) = Q(\overline{k})$, so Q is a constant k-scheme and the result follows. □

Remark 2.4. For every supersingular $j \in \overline{\mathbb{F}}_p$, there is a complete $E/\mathbb{F}_{p^2}$ with $j(E) = j$, see [GL25, §2.3.7].

A final ingredient is the compatibility between the above decomposition of E_n and its ring structure. Making this precise requires uniquely specifying the map π, which we have not done so far.

Lemma 2.5. *Suppose E/k is complete. Choose the map $\pi : E[p] \to \boldsymbol{\alpha}_p$ such that Frobenius is equal to*

$$\iota^{(p)} \circ \pi : E[p] \longrightarrow E^{(p)}[p].$$

Let $u, v \in \mathrm{O}_E$ and let $u_0, v_0 \in k$ be their actions on $\mathrm{Lie}(E[p^n]/k)$. Let S be a k-scheme, then

$$(u + \nu(\beta))(v + \nu(\gamma)) = uv + \nu(u_0\gamma + v_0^p\beta), \qquad \forall\, \beta, \gamma \in \mathrm{End}(\boldsymbol{\alpha}_p/S) \simeq \mathbb{A}^1(S)$$

Proof. Since $u \circ \iota = \iota \circ u_0$, it suffices to show that $\pi \circ v = v_0^p \circ \pi$, so we may assume $n = 1$. We have

$$\begin{aligned}\iota^{(p)} \circ \pi \circ v &= \mathrm{Frob}_{E[p]} \circ v = v^{(p)} \circ \mathrm{Frob}_{E[p]} = v^{(p)} \circ \iota^{(p)} \circ \pi = (v \circ \iota)^{(p)} \circ \pi \\ &= (\iota \circ v_0)^{(p)} \circ \pi = \iota^{(p)} \circ v_0^p \circ \pi,\end{aligned}$$

which implies the conclusion since $\iota^{(p)}$ is a closed immersion. □

2.2. **The moduli problems $\mathcal{C}_{\mathrm{ns}}(p^n)$ and $\mathcal{C}^+_{\mathrm{ns}}(p^n)$.** We introduce non-split Cartan moduli problems, and prove their representability. Henceforth, $\mathbb{Q}_{p^2}$ denotes the quadratic unramified extension of $\mathbb{Q}_p$, with ring of integers $\mathbb{Z}_{p^2}$ and Frobenius automorphism Frob. Fix a $\mathbb{Z}_p$-basis $(1, z)$ of $\mathbb{Z}_{p^2}$, and let

$$f(t) = t^2 + at + b \in \mathbb{Z}_p[t] \tag{13}$$

be the characteristic polynomial of z.

Definition 2.6. *For any elliptic curve E over a scheme S, we let $\mathcal{C}_{\mathrm{ns}}(p^n)(E/S)$ be the set of ring homomorphisms $\mathbb{Z}_{p^2}/(p^n) \to \mathrm{End}_S(E[p^n])$. With the obvious action on morphisms, this defines a functor*

$$\mathcal{C}_{\mathrm{ns}}(p^n) : \underline{\mathbf{Ell}}_{\mathbb{Z}} \longrightarrow \underline{\mathbf{Set}}.$$

Remark 2.7. If R is any ring, assumed unital but not necessarily commutative, and $\alpha : \mathbb{Z}_{p^2}/(p^n) \to R$ is a ring homomorphism, its kernel is of the form $p^k\,\mathbb{Z}_{p^2}/(p^n)$ for some $1 \le k \le n$. If $p^{n-1} \neq 0$ in R, then α is injective and $\alpha \neq \alpha \circ \mathrm{Frob}$. We will repeatedly use this fact in the following two cases:

- $R = \mathrm{End}(E[p^n])$ for some elliptic curve E/S,
- $R = \mathcal{O}/I$, where $\mathcal{O}$ is a quaternion order and I is a two-sided ideal with $p^{n-1} \notin I$.

Proposition 2.8. *The moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$ is relatively representable and affine of finite presentation. It is finite étale above $\mathbb{Z}[1/p]$: for any elliptic curve $E/S/\mathbb{Z}[1/p]$ the map $\mathcal{C}_{\mathrm{ns}}(p^n)_{E/S} \to S$ is finite étale.*

Proof. For any scheme S, there is an obvious bijection between $\mathcal{C}_{\mathrm{ns}}(p^n)(E/S)$ and the set

$$\{u \in \mathrm{End}_S(E[p^n]),\ u^2 + a \cdot u + b \cdot \mathrm{id} = 0\}.$$

The functor $T \mapsto \mathrm{End}_T(E_T[p^n])$ is representable by an affine morphism $X \to S$ of finite presentation [Stu25, Lemma 4.1.4], hence $\mathcal{C}_{\mathrm{ns}}(p^n)$ is relatively representable and affine of finite presentation.

Let S be a scheme, and G be the constant S-group scheme of $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}$. The functor sending T/S to the set of morphisms $\mathbb{Z}_{p^2}/(p^n) \to \mathrm{End}(G_T)$ is represented by the constant S-scheme attached to

$$\{M \in M_2(\mathbb{Z}/p^n\,\mathbb{Z}),\ M^2 + aM + bI_2 = 0\}.$$

Assume now that S is a $\mathbb{Z}[1/p]$-scheme and let E/S be an elliptic curve. Étale-locally over S, the group scheme $E[p^n]$ is isomorphic to the constant group scheme with underlying set $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}$. Hence the S-scheme $\mathcal{C}_{\mathrm{ns}}(p^n)_{E/S}$ is étale-locally (over S) constant, thus the structure map is finite étale. □

Over $\mathbb{Z}[1/p]$ definition 2.6 is the classical notion of non-split Cartan structure. For $N \geq 1$, write $[\Gamma(N)]$ for the set of *Drinfeld bases* of the N-torsion of an elliptic curve (rather than the $\Gamma(N)$-structure of [KM85, (3.1)]). Then $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the *left* on $[\Gamma(N)]$: for a Drinfeld basis $P, Q \in E[N](S)$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (P, Q) = (aP + bQ, cP + dQ), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Lemma 2.9. *Fix a ring homomorphism $\iota : \mathbb{Z}_{p^2}/(p^n) \to M_2(\mathbb{Z}/p^n\mathbb{Z})$, and let $\Gamma_{\mathrm{ns}}(p^n) \leq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be the image of $(\mathbb{Z}_{p^2}/(p^n))^\times$. The morphism $\pi : [\Gamma(p^n)] \to \mathcal{C}_{\mathrm{ns}}(p^n)$ of moduli problems over $\mathbb{Z}[1/p]$, defined by*

$$(P, Q) \in [\Gamma(p^n)](E/S) \;\longmapsto\; \left[z \mapsto \left(\begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \iota(z) \begin{pmatrix} P \\ Q \end{pmatrix} \right) \right] \in \mathcal{C}_{\mathrm{ns}}(p^n)(E/S)$$

factors through an isomorphism

$$[\Gamma(p^n)]/\Gamma_{\mathrm{ns}}(p^n) \xrightarrow{\sim} \mathcal{C}_{\mathrm{ns}}(p^n).$$

Proof. Consider $E/S/\mathbb{Z}[1/p]$ and $(P, Q) \in \Gamma(p^n)(E/S)$. By [KM85, Prop. 1.10.2 (3)], $(a, b) \mapsto aP + bQ$ is an isomorphism between the constant S-group scheme attached to $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}$ and $E[p^n]$, which implies that π is well-defined. Since π is invariant under the action of $\Gamma_{\mathrm{ns}}(p^n)$, it factors through a morphism $\tilde{\pi} : [\Gamma(p^n)]/\Gamma_{\mathrm{ns}}(p^n) \to \mathcal{C}_{\mathrm{ns}}(p^n)$ by [KM85, Theorem 7.1.3], where both sides are finite étale relatively representable. To check that $\tilde{\pi}$ is an isomorphism, it is enough by [Gro67, Corollaire 17.9.5] to check that, for any elliptic curve E over an algebraically closed field k of characteristic prime to p,

$$\pi(E/k) : [\Gamma(p^n)](E/k)/\Gamma_{\mathrm{ns}}(p^n) \to \mathcal{C}_{\mathrm{ns}}(p^n)(E/k)$$

is a bijection, which is straightforward. □

We now turn to the moduli problem attached to *normalisers* of non-split Cartan subgroups.

Definition 2.10. *The group $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathcal{C}_{\mathrm{ns}}(p^n)$ by pre-composing the given ring homomorphism by the Frobenius automorphism of $\mathbb{Z}_{p^2}/(p^n)$. The moduli problem $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ is the quotient of $\mathcal{C}_{\mathrm{ns}}(p^n)$ by $\mathbb{Z}/2\mathbb{Z}$.*

Proposition 2.11. *The moduli problem $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ is well-defined, relatively representable and affine of finite presentation. For any elliptic curve E/S, $\mathcal{C}_{\mathrm{ns}}(p^n)_{E/S}$ is an étale $\mathbb{Z}/2\mathbb{Z}$-torsor over $\mathcal{C}^+_{\mathrm{ns}}(p^n)_{E/S}$ through the forgetful map, which induces an isomorphism*

$$\mathcal{C}_{\mathrm{ns}}(p^n)_{E/S} \,/\, (\mathbb{Z}/2\mathbb{Z}) \;\xrightarrow{\sim}\; \mathcal{C}^+_{\mathrm{ns}}(p^n)_{E/S}.$$

Furthermore, $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ is finite étale over $\mathbb{Z}[1/p]$. The map of lemma 2.9 induces an isomorphism

$$[\Gamma(p^n)] \,/\, \Gamma^+_{\mathrm{ns}}(p^n) \;\xrightarrow{\sim}\; \mathcal{C}^+_{\mathrm{ns}}(p^n).$$

Proof. Let E/S be an elliptic curve and $\alpha : \mathbb{Z}_{p^2}/(p^n) \to \mathrm{End}_S(E[p^n])$ be a ring homomorphism: as we saw, $\alpha \neq \alpha \circ \mathrm{Frob}$, so $\mathbb{Z}/2\mathbb{Z}$ acts freely on $\mathcal{C}_{\mathrm{ns}}(p^n)$. Since $\mathcal{C}_{\mathrm{ns}}(p^n)$ is relatively representable affine of finite presentation, the result follows from [KM85, Theorem 7.1.3]. □

The most interesting features of the moduli problems $\mathcal{C}_{\mathrm{ns}}(p)$ and $\mathcal{C}^+_{\mathrm{ns}}(p)$ appear in characteristic p. The key to the smoothness results of § 2.3 is the following.

Lemma 2.12. *Let E be an elliptic curve over a ring R of characteristic p. Suppose that $\mathcal{C}_{\mathrm{ns}}(p^n)(E/R)$ is not empty. Then the Hasse invariant of E vanishes.*[3]

[3]This is stronger than any base change of E to a field being supersingular, which holds if and only if the Hasse invariant is nilpotent.

Proof. We may assume that $n = 1$, so that there is a ring homomorphism $\iota : \mathbb{F}_{p^2} \to \mathrm{End}(E[p])$. Working Zariski-locally over $\mathrm{Spec}(R)$, by [KM85, (12.4.1.3)] and [SGA3I, Exp. $\mathrm{VII_A}$, §6.1], it is enough to show that the p-Lie algebra structure on $\mathrm{Lie}(E/R)$ is trivial. By lemma 2.1 and [SGA3I, Exp. $\mathrm{VII_A}$, §6.1.1], it suffices to show that the structure of p-Lie algebra on $\mathrm{Lie}(E[p]/R)$ is trivial.

Let $\alpha \in \mathbb{F}_{p^2}$ be the reduction of z, as in (13), then $\iota(\alpha)$ is an endomorphism of $\mathrm{Lie}(E[p]/R) \simeq R$, it acts by multiplication by some $\zeta \in R$ such that $\zeta^2 + a\zeta + b = 0$: in particular, $u + v\alpha \in \mathbb{F}_{p^2} \mapsto u + v\zeta \in R$ is a ring homomorphism. Now, let $x \in \mathrm{Lie}(E[p]/R)$ be a generator, then one has

$$\zeta x^{(p)} = \iota(\alpha)x^{(p)} = (\iota(\alpha)x)^{(p)} = (\zeta x)^{(p)} = \zeta^p x^{(p)}.$$

Because $\alpha - \alpha^p \in \mathbb{F}_{p^2}^\times$, one has $\zeta - \zeta^p \in R^\times$, so $x^{(p)} = 0$ and the conclusion follows. □

Corollary 2.13. *Let $\mathcal{P}$ be the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$ or $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ over $\mathbb{F}_p$. For any $E/S/\mathbb{F}_p$ let $S_0 \subset S$ be the vanishing locus of the Hasse invariant. Then the obvious map of S-schemes is an isomorphism:*

$$\mathcal{P}_{E_{S_0}/S_0} \xrightarrow{\sim} \mathcal{P}_{E/S}\,.$$

Proof. The proof of lemma 2.12 shows S_0 is well-defined. Working étale-locally over S, by proposition 2.11, we may assume S is affine and $\mathcal{P} = \mathcal{C}_{\mathrm{ns}}(p^n)_{\mathbb{F}_p}$. The conclusion follows from lemma 2.12. □

Proposition 2.14. *Let $\mathcal{P}$ denote the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$ or $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ over a perfect field k of characteristic p. Let $\mathcal{L}$ be a finite étale representable moduli problem over k with fine moduli space $\mathcal{M}$ and universal elliptic curve $\mathcal{E}$. Let $H \subset \mathcal{M}$ be the reduced closed subscheme corresponding to the finite set of closed points with supersingular j-invariants, and E/H be the pull-back of $\mathcal{E}\,/\,\mathcal{M}(\mathcal{L})$. Let $q : \mathcal{P}_{E/H} \to H$ be the structure morphism. Then the elliptic curve $(q^*E)/\,\mathcal{P}_{E/H}$ represents the moduli problem $\mathcal{P} \times \mathcal{L}$.*

Proof. Let $\tilde{q} : \mathcal{P}_{\mathcal{E}\,/\,\mathcal{M}} \to \mathcal{M}$, then $(\tilde{q}^*\,\mathcal{E})/\,\mathcal{P}_{\mathcal{E}\,/\,\mathcal{M}}$ represents $\mathcal{P} \times \mathcal{L}$ by [KM85, (4.3.4)]. By corollary 2.13, we only need to show that H is the vanishing locus Z of the Hasse invariant in $\mathcal{M}$. It is enough to check that H and Z are both finite and geometrically reduced k-schemes with the same $\overline{k}$-points. By construction, H is finite reduced; k is perfect so it is geometrically reduced. By [KM85, Theorem 12.4.3], $Z(\overline{k})$ consists exactly of points with supersingular j-invariant, so Z is also finite. Since $\mathcal{L}$ is étale, *loc.cit.* also implies that Z is geometrically reduced. □

This result admits the following more concrete formulation over $k = \overline{\mathbb{F}}_p$.

Corollary 2.15. *Let $\mathcal{P}$ denote the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$ or $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ over $k := \overline{\mathbb{F}}_p$. Let $\mathcal{L}$ be a finite étale representable moduli problem over k. Let $\mathcal{M}(\mathcal{P}, \mathcal{L})$ be the fine moduli scheme attached to the moduli problem $\mathcal{P} \times \mathcal{L}$. Then the classifying map (cf. [KM85, (8.1.3)]) defines an isomorphism*

$$f : \coprod_{(E,z)\in\mathcal{L}^{\mathrm{ss}}} \mathcal{P}_{E/k} \xrightarrow{\sim} \mathcal{M}(\mathcal{P}, \mathcal{L}),$$

where $\mathcal{L}^{\mathrm{ss}}$ is the finite set of isomorphism classes of (E, z), where E/k is supersingular and $z \in \mathcal{L}(E/k)$.

It remains to understand the scheme $\mathcal{C}_{\mathrm{ns}}(p^n)_{E/k}$ where E/k is a complete supersingular curve. Define an action of $\underline{\mathrm{End}}(\boldsymbol{\alpha}_p)$ on $\mathcal{C}_{\mathrm{ns}}(p^n)_{E/k}$ as follows: for any k-algebra R, there is a canonical bijection between $\mathcal{C}_{\mathrm{ns}}(p^n)(E/R)$ and $\{\phi \in \mathrm{End}(E[p^n]_R) : f(\phi) = 0\}$ with f as in (13). For any $\lambda \in \mathrm{End}(\boldsymbol{\alpha}_p/R)$ set

$$\lambda \star \phi := \phi + \nu(\lambda) \quad \in \mathrm{End}(E[p^n]_R).$$

Note that $f(\lambda \star \phi) = 0$: By lemma 2.5 and proposition 2.3 it suffices to show that $\phi_0 + \phi_0^p \equiv -a \pmod p$ for any $\phi \in \mathrm{End}(E)$ satisfying $f(\phi) = 0$. This holds since $f(\phi_0) = 0$ by lemma 2.1 so that $\phi_0 \in \mathbb{F}_{p^2}$ and

$$t^2 + at + b = (t - \phi_0)(t - \phi_0^p) \quad \text{in } k[t]. \tag{14}$$

The following is a consequence of the results above.

Proposition 2.16. *Let E/k be a complete supersingular curve. There is an $\underline{\mathrm{End}}(\boldsymbol{\alpha}_p)$-equivariant isomorphism*

$$\rho : \mathcal{C}_{\mathrm{ns}}(p^n)_{E/k} \xrightarrow{\sim} \coprod_{u:\mathbb{Z}_{p^2}/(p^n)\to R_n(E)} \underline{\mathrm{End}}(\boldsymbol{\alpha}_p)$$

sending a ring homomorphism $u : \mathbb{Z}_{p^2}/(p^n) \to \mathrm{End}(E[p^n]_{\overline{k}})$ to the component indexed by the projection of u modulo the unit component of $\underline{\mathrm{End}}_k(E[p^n])$. The action of $\mathbb{Z}/2\mathbb{Z}$ satisfies:

- *it acts on the index set by pre-composing with Frobenius, so that it has no fixed point on $\pi_0(\mathcal{C}_{\mathrm{ns}}(p^n)_{E/k})$.*
- *it* reverses *the $\underline{\mathrm{End}}(\boldsymbol{\alpha}_p)$-action: for $\lambda \in \underline{\mathrm{End}}(\boldsymbol{\alpha}_p)(\overline{k})$ and $u \in \mathcal{C}_{\mathrm{ns}}(p^n)_{E/k}(\overline{k})$, one has*

$$\overline{1} \cdot (\lambda \star u) = (-\lambda) \star (\overline{1} \cdot u).$$

In particular, $\mathcal{C}^+_{\mathrm{ns}}(p^n)_{E/k}$ is isomorphic to the disjoint union of p^{2n-2} copies of $\mathbb{A}^1_k$.

Proof. This follows from propositions 2.2 and 2.3. For the final claim, restrict ρ^{-1} to a subset of components corresponding to a set of representatives for morphisms $\mathbb{Z}_{p^2}/(p^n) \to R_n(E)$ modulo pre-composition by Frobenius, and use proposition 2.11. For the component count, one can check that $R_n(E)^\times$ acts transitively on its subrings $R \simeq \mathbb{Z}_{p^2}/(p^n)$ and that the stabiliser of a given R is $R^\times$, and then apply [Voi21, Lemma 26.6.7] to the preimage of R in O_E. □

Corollary 2.17. *Let k be a field of characteristic p and $\mathcal{L}$ a finite étale representable moduli problem over k. Then the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n) \times \mathcal{L}$ (resp. $\mathcal{C}^+_{\mathrm{ns}}(p^n) \times \mathcal{L}$) is representable by a smooth affine scheme of relative dimension one. If k is algebraically closed, this scheme is the disjoint union of copies of $\mathbb{A}^1_k$ indexed by the k-isomorphism classes of (E, u, z) (resp. (E, R, k)), where E/k is supersingular, $u : \mathbb{Z}_{p^2}/(p^n) \to R_n(E)$ is a ring homomorphism (resp. $R \subset R_n(E)$ a subring isomorphic to $\mathbb{Z}_{p^2}/(p^n)$), and $z \in \mathcal{L}(E/k)$.*

Proof. Since smoothness of relative dimension one can be tested fpqc-locally on the base, we may assume that k is algebraically closed. The claim then follows from the previous results. □

Proposition 2.18. *Let R be any ring and $\mathcal{L}$ be a finite étale representable moduli problem over R. Then the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n) \times \mathcal{L}$ (resp. $\mathcal{C}^+_{\mathrm{ns}}(p^n) \times \mathcal{L}$) is representable by a R-scheme which is affine and smooth of relative dimension one over R.*

Proof. By [KM85, (4.12)] we may assume that $\mathcal{L} = [\Gamma_1(N)]$ over $R = \mathbb{Z}[1/N]$ for $N \geq 4$. By previous results and [Stu25, Prop. 1.3.4], since smoothness can be tested fpqc-locally on the base, we may even assume that $\mathcal{L} = [\Gamma_1(N)]$ over $R = W(\overline{\mathbb{F}}_p)$ for $N \geq 4$ prime to p. The fine moduli scheme $\mathcal{M}$ attached to $\mathcal{C}_{\mathrm{ns}}(p^n) \times \mathcal{L}$ (resp. $\mathcal{C}^+_{\mathrm{ns}}(p^n) \times \mathcal{L}$) exists and is affine; we wish to show that it is smooth of relative dimension one over R. This holds for its generic fibre (the moduli problem is finite étale representable), which is irreducible (by considering the complex uniformization). It also holds for the special fibre by corollary 2.17. By [Stu25, Prop. 4.3.4], it is enough to show that every connected component of the special fibre of $\mathcal{M}$ contains the specialisation of some R-point of $\mathcal{M}$.

By our description of the special fibre of $\mathcal{M}$ and since $\mathcal{L}$ is étale, it is enough to show the following: for every supersingular elliptic curve $E_0/\overline{\mathbb{F}}_p$ and every ring homomorphism $u : \mathbb{Z}_{p^2}/(p^n) \to R_n(E_0)$, there exists an elliptic curve E/R, an isomorphism $g : E_0 \to E_{\overline{\mathbb{F}}_p}$ such that

$$\mathrm{End}(E) \xrightarrow{g} \mathrm{End}(E_0) \longrightarrow R_n(E_0)$$

has the same image as u. This can be shown by a direct adaptation of [GZ85, Proposition 2.7]. □

2.3. **Smoothness of the coarse moduli scheme.** We now turn to removing the auxiliary level structure, and study the coarse moduli scheme associated to $\mathcal{C}_{\mathrm{ns}}(p^n)$ and $\mathcal{C}^+_{\mathrm{ns}}(p^n)$.

Lemma 2.19. *Let E/k be a complete supersingular elliptic curve, $\phi \in \mathrm{Aut}(E/k)\backslash\{\pm 1\}$, and define*

$$Y := \mathcal{C}_{\mathrm{ns}}(p^n)_{E/k} \qquad Y^+ := \mathcal{C}^+_{\mathrm{ns}}(p^n)_{E/k}.$$

Then ϕ has finitely many fixed points in $Y(\overline{k})$ and $Y^+(\overline{k})$. Furthermore, every element of $\pi_0(Y^+/\overline{k})$, resp. $Y^+(\overline{k})$, that is fixed by ϕ is the image of an element of $\pi_0(Y/\overline{k})$, resp. $Y(\overline{k})$, fixed by ϕ.

Proof. Fix a $\mathbb{Z}_p$-basis $(1, z)$ of $\mathbb{Z}_{p^2}$, then Y is endowed with an action of $\underline{\mathrm{End}}(\boldsymbol{\alpha}_p)$, and the connected components of Y and Y^+ are geometrically connected, see proposition 2.16.

Let $\phi_0 \in k$ be the action of ϕ on $\mathrm{Lie}(E/k)$. Since $\phi\phi^\vee = 1$ it follows from (14) that $\phi_0^{p+1} = 1$. Let $u : \mathbb{Z}_{p^2}/(p^n) \to R_n(E)$ be a ring homomorphism such that $\phi u \phi^{-1} = u \circ \mathrm{Frob}^r$ with $r \in \{0, 1\}$. Since $\mathrm{O}_E/\mathfrak{P}_E$ is commutative, $u = \phi u \phi^{-1}$ modulo $\mathfrak{P}_E$, and in particular $u(z - \mathrm{Frob}^r(z)) \in \mathfrak{P}_E$. Hence $z - \mathrm{Frob}^r(z) \notin \mathbb{Z}_{p^2}^\times$, thus $r = 0$. Hence, if $x \in \pi_0(Y^+)$ is fixed by ϕ, then x is the image of $y \in \pi_0(Y)$ fixed by ϕ. Likewise, if $x \in Y^+(\overline{k})$ is fixed by ϕ, then it is the image of some $y \in Y(\overline{k})$ fixed by ϕ.

Let $u : \mathbb{Z}_{p^2}/(p^n) \to \mathrm{O}_E/(p^n) \subset \mathrm{End}(E[p^n])$ be a ring homomorphism that commutes with ϕ modulo $p^{n-1}\mathfrak{P}_E$, so the connected component of u in Y is stable under ϕ. For any $\lambda \in \mathrm{End}(\boldsymbol{\alpha}_p/\overline{k})$ we have

$$\phi \cdot (\lambda \star u) = \phi_0^2 \lambda \star \phi u \phi^{-1}.$$

If p is inert in the order $\mathbb{Z}[\phi]$, then $\phi_0^2 \neq 1$, so ϕ has exactly one fixed point in the connected component of u in Y. Otherwise, either $p = 2$ and ϕ has order 4, or $p = 3$ and ϕ has order 3 or 6. In either case $\phi_0^2 = 1$, so ϕ acts on the connected component of u as a translation. In particular, if $\phi u \phi^{-1} \neq u$, then ϕ has no fixed point on the connected component of u. Suppose $\phi u \phi^{-1} = u$, then a calculation in $\mathrm{O}_E/(p)$ shows that $u(z) - c$ is nilpotent for some $c \in \mathbb{F}_p$. This is impossible since $(1, z)$ is a $\mathbb{Z}_p$-basis of $\mathbb{Z}_{p^2}$. □

The following results conclude the proof of theorem A. Let us say that a moduli problem $\mathcal{L}$ over a ring R is *symmetric* if, for every elliptic curve $E/S/R$, the automorphism -1 of E acts trivially on $\mathcal{L}(E/R)$. Note that $\mathcal{C}_{\mathrm{ns}}(p^n)$ and $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ are symmetric for any $n \geq 1$, as is $[\Gamma(N)]/\Gamma$ for any $\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $\pm I_2$. Any finite product of symmetric moduli problems is also symmetric.

Proposition 2.20. *Let R be a regular ring, $\mathcal{L}$ a finite étale symmetric relatively representable moduli problem over R, and $\mathcal{P}$ the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$ or $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ over R. Then $\mathcal{P} \times \mathcal{L}$ has a coarse moduli scheme $\mathrm{M}(\mathcal{P} \times \mathcal{L})$ over R, which is smooth of relative dimension 1 and satisfies coarse base change to regular rings.*

Proof. The coarse moduli scheme $M = \mathrm{M}(\mathcal{P} \times \mathcal{L})$ exists by [KM85, (8.1.1)], since $\mathcal{P} \times \mathcal{L}$ is relatively representable and affine. To check the other claims, we may work Zariski-locally on R and assume that some integer $N \geq 3$ is invertible on R. Then the moduli scheme $\mathcal{M} := \mathcal{M}(\mathcal{P} \times \mathcal{L} \times [\Gamma(N)])$ is a smooth affine R-scheme of relative dimension one by proposition 2.18. It carries an action of the group $G := \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm\mathrm{id}\}$ because $\mathcal{L}$ is symmetric, and one has $M = \mathcal{M}/G$.

The smoothness of M follows from the first theorem in the Notes of Chapters 8 and 10 (p. 508) of [KM85]. To check coarse base change along morphisms of regular rings, we wish to apply the theorem on p. 510 of [KM85]: one has to check that, for every non-unit $g \in G$, every geometric fibre of $\mathcal{M} \to \mathrm{Spec}\, R$ has finitely many fixed points under g.

It is enough to show that, if k is an algebraically closed field, there are finitely many isomorphism classes of (E, α) (where E/k is an elliptic curve and $\alpha \in \mathcal{P}(E/k)$) such that E admits an automorphism j (which is not $\pm\mathrm{id}$) preserving α. If p is invertible in k, $\mathcal{P}$ is finite étale and $\mathrm{Aut}(E)^\times = \{\pm 1\}$ unless $j(E) \in \{0, 1728\}$, so this is clear. Otherwise, this follows from lemma 2.19. □

Corollary 2.21. *Let R be a DVR with residue field k of characteristic p. Let $\mathcal{P}$ be the moduli problem $\mathcal{C}_{\mathrm{ns}}(p^n)$, resp. $\mathcal{C}^+_{\mathrm{ns}}(p^n)$, and $\mathcal{L}$ a finite étale symmetric relatively representable moduli problem over R. The geometric special fibre of the coarse moduli scheme $\mathrm{M}(\mathcal{P}\times\mathcal{L})$ is the disjoint union of copies of $\mathbb{A}^1$ indexed by the isomorphism classes of (E,u,α), resp. (E,A,α), where $E/\overline{k}$ is a supersingular elliptic curve, $u:\mathbb{Z}_{p^2}/(p^n)\to R_n(E)$ is a ring homomorphism, resp. $A\subset R_n(E)$ is a subring isomorphic to $\mathbb{Z}_{p^2}/(p^n)$, and $\alpha\in\mathcal{L}(E/\overline{k})$.*

Proof. By proposition 2.20, the special fibre (resp. geometric special fibre) of $\mathrm{M}(\mathcal{P}\times\mathcal{L})$ is the coarse moduli scheme attached to the base-changed moduli problem $\mathcal{P}\times\mathcal{L}$ over k (resp. $\overline{k}$) and it is smooth of relative dimension one. We may thus assume that $R=k$.

By corollary 2.13 and [KM85, Lem. 8.1.3.1], the set-theoretic image of the j-invariant $\mathrm{M}(\mathcal{P}\times\mathcal{L})\to\mathbb{A}^1_k$ is contained in the finite set $\mathcal{S}$ of supersingular j-invariants; $\mathrm{M}(\mathcal{P}\times\mathcal{L})$ is geometrically reduced, so the scheme-theoretic image of j is the reduced closed subscheme of $\mathbb{A}^1_k$ attached to $\mathcal{S}$. By corollary 2.13 and [KM85, Cor. 12.4.4], if $E/\overline{k}$ is supersingular with universal formal deformation $\mathcal{E}/\overline{k}[\![t]\!]$, then $(\mathcal{P}\times\mathcal{L})_{\mathcal{E}/\overline{k}[\![t]\!]}$ is isomorphic over $\overline{k}[\![t]\!]$ to $(\mathcal{P}\times\mathcal{L})_{E/\overline{k}}$, where $\overline{k}$ is viewed as $\overline{k}[\![t]\!]/(t)$, compatible with the action of $\mathrm{Aut}(E)$. Therefore, by [KM85, Prop 8.2.3], the classifying map induces an isomorphism

$$\coprod_{\substack{E/\overline{k}\\ \alpha\in\mathcal{L}(E/\overline{k})'}} \frac{\mathcal{P}_{E/\overline{k}}}{\mathrm{Aut}(E,\alpha)/\{\pm\mathrm{id}\}} \xrightarrow{\sim} \mathrm{M}(\mathcal{P}\times\mathcal{L})_{\overline{k}},$$

where $\mathcal{L}(E/\overline{k})'$ denotes a system of representatives for $\mathcal{L}(E/\overline{k})$ modulo $\mathrm{Aut}(E)$. Each $\mathcal{P}_{E/\overline{k}}$ is a union of copies of $\mathbb{A}^1_k$ indexed by morphisms $\mathbb{Z}_{p^2}/(p^n)\to R_n(E)$ (resp. subrings of $R_n(E)$ isomorphic to $\mathbb{Z}_{p^2}/(p^n)$), and this identification is compatible with $\mathrm{Aut}(E)$. The result follows, since over any field the quotient of $\mathbb{A}^1$ by a finite group is isomorphic to $\mathbb{A}^1$, see for instance [KM77, Lemma 3.2.1]. □

Remark 2.22. The number of components of $\mathscr{X}^+_{\mathrm{ns}}(p^n)_{\overline{\mathbb{F}}_p}$ can be found by considering, for each supersingular elliptic curve $E/\overline{\mathbb{F}}_p$, the action of $\mathrm{Aut}(E)$ on the p^{2n-2} components of $\mathcal{C}^+_{\mathrm{ns}}(p^n)_{E/k}$ (proposition 2.16).

Corollary 2.23. *The coarse moduli scheme $\mathscr{X}^+_{\mathrm{ns}}(p)$ attached to the moduli problem $\mathcal{C}^+_{\mathrm{ns}}(p)$ over $\mathbb{Z}$ exists. It is smooth affine, and has a j-invariant map to $\mathbb{A}^1_{\mathbb{Z}}$. The fibre $\mathscr{X}^+_{\mathrm{ns}}(p)_{\mathbb{F}_p}$ is the disjoint union of the $j^{-1}(s)\simeq\mathbb{A}^1_{\kappa(s)}$, where $s\in\mathbb{A}^1_{\mathbb{F}_p}$ runs over the supersingular points.*

Proof. The j-invariant $j:\mathscr{X}^+_{\mathrm{ns}}(p)_{\mathbb{F}_p}\to\mathbb{A}^1_{\mathbb{F}_p}$ has scheme-theoretic image equal to the reduced subscheme of the supersingular locus (because the source is smooth). We need to show that for every supersingular $s\in\mathbb{A}^1_{\mathbb{F}_p}$, the fibre $X_s:=j^{-1}(s)$ is isomorphic to $\mathbb{A}^1_{\kappa(s)}$. By corollary 2.21 this holds geometrically, so the result follows since all forms of $\mathbb{A}^1_k$ over a perfect field k are trivial [Rus70, Lemma 1.1]. □

2.4. **Moduli scheme for mixed Cartan structures.** We now introduce mixed Cartan problems and the associated moduli schemes. They are defined prime by prime, so all that remains to do is introduce the moduli problem attached to the normaliser of a split Cartan subgroup.

Definition 2.24. *For any prime power p^n, define the moduli problems $\mathcal{C}_{\mathrm{sp}}(p^n)$ and $\mathcal{C}^+_{\mathrm{sp}}(p^n)$ over $\mathbb{Z}$ as the quotient of $[\Gamma(p^n)]_{\mathbb{Z}}$ by the subgroups $\Gamma_{\mathrm{sp}}(p^n)$ and $\Gamma^+_{\mathrm{sp}}(p^n)$ of diagonal matrices, resp. diagonal or anti-diagonal matrices, in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Given two coprime positive integers $N_{\mathrm{sp}},N_{\mathrm{ns}}$, we define*

$$\mathcal{C}(N_{\mathrm{sp}},N_{\mathrm{ns}}):=\prod_{p^k\|N_{\mathrm{sp}}}\mathcal{C}_{\mathrm{sp}}(p^k)\times\prod_{p^k\|N_{\mathrm{ns}}}\mathcal{C}_{\mathrm{ns}}(p^k),\qquad \mathcal{C}^+(N_{\mathrm{sp}},N_{\mathrm{ns}}):=\prod_{p^k\|N_{\mathrm{sp}}}\mathcal{C}^+_{\mathrm{sp}}(p^k)\times\prod_{p^k\|N_{\mathrm{ns}}}\mathcal{C}^+_{\mathrm{ns}}(p^k)$$

Proposition 2.25. *The moduli problems $\mathcal{C}(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ and $\mathcal{C}^+(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ are relatively representable, affine, smooth above $\mathbb{Z}[1/N_{\mathrm{sp}}]$, finite above $\mathbb{Z}[1/N_{\mathrm{ns}}]$, and admit coarse moduli schemes*

$$\mathscr{X}_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}}), \qquad \mathscr{X}^+_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}})$$

over $\mathbb{Z}$. These schemes are affine, normal, of finite type and flat of relative dimension one over $\mathbb{Z}$. They are smooth over $\mathbb{Z}[1/N_{\mathrm{sp}}]$ and their formation commutes with base change to regular $\mathbb{Z}[1/N_{\mathrm{sp}}]$-algebras.

Proof. By [KM85, Theorem 5.1.1, Theorem 7.1.3], one sees that $\mathcal{C}_{\mathrm{sp}}(p^n), \mathcal{C}^+_{\mathrm{sp}}(p^n)$ are relatively representable, symmetric, finite and normal. They are étale above $\mathbb{Z}[1/p]$. The statement follows from our previous results on non-split Cartan moduli problems and results of [KM85], namely Theorem 5.1.1, Theorem 7.1.3, §8.1 and Proposition 8.2.2. □

Remark 2.26. The curves $\mathscr{X}_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}})_{\mathbb{Q}}$ and $\mathscr{X}^+_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}})_{\mathbb{Q}}$ are the non-cuspidal loci of the Cartan modular curves described in [DLM22, §3]. They are respectively attached to Cartan and Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/N_{\mathrm{sp}}N_{\mathrm{ns}}\mathbb{Z})$ in the terminology of *loc.cit.*.

Definition 2.27. *Let $N \geq 1$ be an integer and A be an étale free $\mathbb{Z}/N\mathbb{Z}$-algebra of rank two. Let N_{sp} be the product of the primes $p \mid N$ at which A splits. Given an elliptic curve $E/S/\mathbb{Z}[1/N_{\mathrm{sp}}]$, we say that a ring homomorphism*

$$f : A \longrightarrow \mathrm{End}_S(E[N])$$

is regular *if for every $a \in A\backslash\{0\}$ and every $s \in S$, the endomorphism $f(a)_s$ of $E_s[N]$ is non-zero. For any elliptic curve $E/S/\mathbb{Z}[1/N_{\mathrm{sp}}]$, let $\mathcal{P}_A(E/S)$ be the set of regular homomorphisms $A \to \mathrm{End}_S(E[N])$. The group $\mathrm{Aut}(A)$ acts (on the right) by pre-composition on the moduli problem $\mathcal{P}_A$ over $\mathbb{Z}[1/N]$.*

We also need a variant of lemma 2.9 for the mixed Cartan moduli problems.

Lemma 2.28. *Let p be a prime and $n \geq 1$. The moduli problem $\mathcal{P} := \mathcal{P}_{(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}}$ is relatively representable and finite étale. The morphism of moduli problems $\pi : [\Gamma(p^n)] \to \mathcal{P}$ defined by*

$$(P,Q) \in [\Gamma(p^n)](E/S) \mapsto \left[(z_1,z_2) \in (\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2} \mapsto \left(\begin{pmatrix} P \\ Q \end{pmatrix} \mapsto \begin{pmatrix} z_1 P \\ z_2 Q \end{pmatrix}\right)\right] \in \mathcal{P}(E/S)$$

is well-defined and factors through an isomorphism $\mathcal{C}_{\mathrm{sp}}(p^n) \simeq \mathcal{P}$. Pre-composing with the involution

$$(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2} \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2} : (x,y) \longmapsto (y,x),$$

defines an action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathcal{P}$. The quotient $\mathcal{P}^+ := \mathcal{P}/(\mathbb{Z}/2\mathbb{Z})$ is well-defined over $\mathbb{Z}[1/p]$, relatively representable and finite étale. Composing π with $\mathcal{P} \to \mathcal{P}^+$ induces an isomorphism $\mathcal{C}^+_{\mathrm{sp}}(p^n) \simeq \mathcal{P}^+$.

Proof. To show the relative representability and that $\mathcal{P}_{(\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}}$ is finite étale, it is enough to show by étale descent that if E is an elliptic curve over some $\mathbb{Z}[1/p]$-scheme S and $E[p^n]$ is a constant S-scheme, then $\mathcal{P}_{E/S}$ exists and is a finite étale S-scheme, which is a direct verification. The rest is proved in a similar way to lemma 2.9 and proposition 2.11. □

Let $N_{\mathrm{ns}}, N_{\mathrm{sp}}$ be two coprime positive integers and $N = N_{\mathrm{ns}} \cdot N_{\mathrm{sp}}$. Let A be the quadratic étale $\mathbb{Z}/N\mathbb{Z}$-algebra that is split at prime divisors of N_{sp}, and nonsplit at prime divisors of N_{ns}, i.e.

$$A = A(N_{\mathrm{sp}}, N_{\mathrm{ns}}) := \Big(\prod_{p^k \| N_{\mathrm{spl}}} (\mathbb{Z}/p^k\mathbb{Z})^2\Big) \times \Big(\prod_{p^k \| N_{\mathrm{ns}}} \mathbb{Z}_{p^2}/p^k\mathbb{Z}_{p^2}\Big). \tag{15}$$

Corollary 2.29. *The moduli problem $\mathcal{P}_A$ is relatively representable, affine of finite presentation, and naturally isomorphic to $\mathcal{C}(N_{\mathrm{sp}}, N_{\mathrm{ns}})_{\mathbb{Z}[1/N_{\mathrm{sp}}]}$. The group $(\mathbb{Z}/2\,\mathbb{Z})^t$ acts on $\mathcal{P}_A$, generated by pairwise-commuting involutions σ_p for each $p \mid N$, where σ_p acts by the Frobenius involution on $\mathbb{Z}_{p^2}/(p^k)$ if $p \mid N_{\mathrm{ns}}$, and by swapping the elements of the idempotent basis of $(\mathbb{Z}/p^k\,\mathbb{Z})^2$ if $p \mid N_{\mathrm{sp}}$. The quotient moduli problem $\mathcal{P}_A^+ := \mathcal{P}_A/(\mathbb{Z}/2\,\mathbb{Z})^t$ exists, is relatively representable, affine of finite presentation, and is isomorphic to $\mathcal{C}^+(N_{\mathrm{sp}}, N_{\mathrm{ns}})_{\mathbb{Z}[1/N_{\mathrm{sp}}]}$.*

Proof. This follows from prime factorization [KM85, Propositions 1.8.2, 3.5.1] and the following simpler variant of Prop. 7.3.1 of *op.cit.* (which does not apply since $\mathcal{C}_{\mathrm{ns}}(p^n)$ or $\mathcal{C}^+_{\mathrm{ns}}(p^n)$ are not flat). Let $\mathcal{P}_1, \mathcal{P}_2$ be two moduli problems over $\underline{\mathbf{Ell}}_{\mathbb{Z}[1/N_{\mathrm{sp}}]}$ that are relatively representable affine and G_1, G_2 be finite groups acting *freely* on $\mathcal{P}_1, \mathcal{P}_2$ respectively. Then the natural map

$$(\mathcal{P}_1 \times \mathcal{P}_2)/(G_1 \times G_2) \longrightarrow (\mathcal{P}_1/G_1) \times (\mathcal{P}_2/G_2)$$

is an isomorphism. Given the construction of the quotient moduli problem (cf. [KM85, pp. 190–191]), one reduces this claim to its commutative algebra analogue, which follows from [KM85, Cor. A7.1.2]. □

2.5. **Minimal regular compactifications of $\mathscr{X}^+_{\mathrm{ns}}(p)$.** Edixhoven–Parent [EP24] construct a minimal regular model $X_{\mathrm{EP}}(p)$ for the modular curve $X^+_{\mathrm{ns}}(p)$ over $W := W(\overline{\mathbb{F}}_p)$ when $p \geq 11$. We will now compare the coarse moduli scheme $\mathscr{X}^+_{\mathrm{ns}}(p)$ over W with $X_{\mathrm{EP}}(p)$. There is an obvious difference between the two schemes: $X_{\mathrm{EP}}(p)$ is proper and has non-smooth points over W, whereas $\mathscr{X}^+_{\mathrm{ns}}(p)$ is affine and smooth over W. We show that this is essentially the only difference: $\mathscr{X}^+_{\mathrm{ns}}(p)$ is identified with the smooth locus of $X_{\mathrm{EP}}(p)$. For $p < 11$ the modular curve $X^+_{\mathrm{ns}}(p)$ has genus 0 so there is no unique minimal regular model. In these cases, we instead exhibit $\mathscr{X}^+_{\mathrm{ns}}(p)$ as an open subscheme of $\mathbb{P}^1_{\mathbb{Z}}$.

The following lemma is well-known to experts, similar arguments appear for instance in Zywina [Zyw15, Prop. 1.13], Le Fourn–Lemos [FL21, Appendix B], as well as the recent works of Furio–Lombardo [FL25, Chapter 3], Bisatt–Furio–Lombardo [BFL26, Theorem 1.3] and Rebolledo–Wuthrich [RW25, Prop. 4].

Lemma 2.30. *Let $K/\mathbb{Q}_p$ be a finite extension with ramification index $e < p-1$ and let E/K be an elliptic curve such that $\mathcal{C}_{\mathrm{ns}}(p)(E/K)$ is not empty. Then E has potentially good reduction. If E has good reduction, then this reduction is supersingular and $\mathcal{C}_{\mathrm{ns}}(p)(E/K)$ contains exactly two elements.*

Proof. Because $\mathcal{C}_{\mathrm{ns}}(p)(E/K) \neq \emptyset$, the image of

$$\rho_{E,p} : G_K := \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[p](\overline{K})) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

is contained in a non-split Cartan subgroup. Suppose $j(E) \notin \mathcal{O}_K$, then by Tate uniformization the mod p cyclotomic character is trivial on the inertia subgroup of K, which contradicts $e < p-1$.

Assume $\mathcal{E}/\mathcal{O}_K$ is an elliptic curve with $\mathcal{E}_K \simeq E$. Then $\mathcal{C}_{\mathrm{ns}}(p)(\mathcal{E}/\mathcal{O}_K) \neq \emptyset$ by Raynaud [Ray74, (3.3.3), (3.3.6)], so the Hasse invariant of $\mathcal{E}_{\mathcal{O}_K/(p)}$ vanishes by lemma 2.12. Serre [Ser72, Prop. 10(b)] showed that the inertia subgroup of G_K has image eC under $\rho_{E,p}$, where $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ is a non-split Cartan subgroup. Since $e < p-1$, this image is non-scalar, so $\mathcal{C}_{\mathrm{ns}}(p)(E/K)$ contains one $\mathbb{Z}/2\mathbb{Z}$-orbit. □

We now show that for $p \geq 11$, $\mathscr{X}^+_{\mathrm{ns}}(p)$ satisfies a weak form of the Néron model property.

Proposition 2.31. *Let $p \geq 11$ be prime and $K/\mathbb{Q}_p$ be finite unramified. The j-map $\mathscr{X}^+_{\mathrm{ns}}(p)(K) \to \mathcal{O}_K$ is well-defined and injective, and the obvious map induces a bijection*

$$\mathscr{X}^+_{\mathrm{ns}}(p)(\mathcal{O}_K) \xrightarrow{\sim} \mathscr{X}^+_{\mathrm{ns}}(p)(K).$$

Proof. We will show that every $P \in X^+_{\mathrm{ns}}(p)(K)$ comes from the image under the classifying map of some (E, u) with $u \in \mathcal{C}_{\mathrm{ns}}(p)(\mathcal{E}_L/L)$, where L/K has ramification index $e \leq 6$ and $\mathcal{E}/\mathcal{O}_L$ is an elliptic

curve. By Raynaud's theorem [Ray74, (3.3.3),(3.3.6)], $\mathcal{C}_{\mathrm{ns}}(p)(\mathcal{E}_L/L) \simeq \mathcal{C}_{\mathrm{ns}}(p)(\mathcal{E}/\mathcal{O}_L)$, so P extends to $\mathscr{X}^+_{\mathrm{ns}}(p)(\mathcal{O}_L)$. Since $\mathscr{X}^+_{\mathrm{ns}}(p)$ is affine, P extends to $\mathscr{X}^+_{\mathrm{ns}}(p)(\mathcal{O}_L \cap K) = \mathscr{X}^+_{\mathrm{ns}}(p)(\mathcal{O}_K)$ and we are done.

Let E/K be an elliptic curve with $j(E) \neq 0, 1728$. Then the set of $z \in X^+_{\mathrm{ns}}(p)(\overline{K})$ with $j(z) = j(E)$ identifies with $\mathcal{C}^+_{\mathrm{ns}}(p)(E/\overline{K})$ as $\mathrm{Gal}(\overline{K}/K)$-sets. Let $P, Q \in X^+_{\mathrm{ns}}(p)(\overline{K})$ be such that $j(P) = j(Q) = j(E)$. Let K'/K be the compositum of the quadratic extensions of K (which has ramification index 2), then P, Q correspond to $u, v \in \mathcal{C}_{\mathrm{ns}}(p)(E_{K'}/K')$. In particular, $E_{K'}$ has potentially good reduction. Therefore, there exists L_1/K with ramification index in $\{1, 2, 3, 4, 6\}$ such that E_{L_1} has good reduction. Let $L = L_1K$, it has ramification index $e \in \{2, 4, 6\}$. Since $\mathcal{C}_{\mathrm{ns}}(p)(E_{K'/K}) \subset \mathcal{C}_{\mathrm{ns}}(p)(E_L/L)$, u and v are in the same $\mathbb{Z}/2\mathbb{Z}$-orbit so $P = Q$.

Let E/K be an elliptic curve with good reduction such that $\mathrm{Aut}(E)$ has $2w$ elements with $w \in \{2, 3\}$. Then the set of $z \in X^+_{\mathrm{ns}}(p)(\overline{K})$ such that $j(z) = j(E)$ identifies with $\mathcal{C}^+_{\mathrm{ns}}(p)(\overline{K})/\mathrm{Aut}(E)$ as a G_K-set.

Let $P \in X^+_{\mathrm{ns}}(p)(K)$ with $j(P) = j(E)$. Then P corresponds to $u \in \mathcal{C}_{\mathrm{ns}}(p)(E_L/L)$ for some extension L/K with degree at most $2w < p-1$. Hence E has supersingular reduction and p is inert in the quadratic ring $\mathrm{End}(E)$. Therefore, $\mathcal{C}_{\mathrm{ns}}(p)(E/K)$ contains a morphism $u_0 : \mathbb{F}_{p^2} \simeq \mathrm{End}(E)/(p) \to \mathrm{End}(E[p])$, so u is in the same $\mathbb{Z}/2\mathbb{Z}$-orbit as u_0, so P is the corresponding Heegner point, which clearly extends. □

Proposition 2.32. *Let p be a prime number. There exists an open immersion*

$$\mathscr{X}^+_{\mathrm{ns}}(p) \longrightarrow X$$

where X is a (relatively) minimal model over $\mathbb{Z}$ of $X^+_{\mathrm{ns}}(p)_{\mathbb{Q}}$. When $p \geq 11$, the image of this open immersion is the smooth, non-cuspidal locus of X. When $p \leq 7$, there is an abstract isomorphism $X \simeq \mathbb{P}^1_{\mathbb{Z}}$.

Proof. Let $Y = \mathscr{X}^+_{\mathrm{ns}}(p)$ for simplicity. Since Y is affine, Y is an open subscheme of some proper $\mathbb{Z}$-scheme X. Replacing X with the scheme-theoretic image of Y in X, we may assume that X is integral, flat over $\mathbb{Z}$, and of dimension 2 (cf. [Gro66, Proposition 13.2.10, Remarque 13.2.12]). Replacing X with its normalization (possible by [Gro65, Scholie 7.8.3] and since Y is normal), we may assume that X is normal. Since Y is regular, by Lipman's theorem [Art86, Theorem 1.1], we may assume that X is regular. In conclusion, there is an open immersion $Y \to X$ such that X is regular connected of dimension 2 and proper flat over $\mathbb{Z}$: in particular, the geometric fibres of $X \to \mathrm{Spec}(\mathbb{Z})$ are connected.

Since $X_{\mathbb{Q}}$ is normal projective over $\mathbb{Q}$, it is isomorphic to $X^+_{\mathrm{ns}}(p)_{\mathbb{Q}}$. The results of [KM85, § 10] imply that $X^+_{\mathrm{ns}}(p)_{\mathbb{Q}}$ extends to a smooth proper curve X^{KM} over $\mathbb{Z}[1/p]$ with geometrically connected fibres. The isomorphism $X_{\mathbb{Q}} \simeq X^+_{\mathrm{ns}}(p)_{\mathbb{Q}}$ extends over $\mathbb{Z}[1/Np]$ for some $N \geq 1$ prime to p by [Gro66, Théorème 8.10.5], and we may glue $X_{\mathbb{Z}[1/N]}$ to $X^{\mathrm{KM}}_{\mathbb{Z}[1/p]}$: this scheme is regular, connected, flat, proper over $\mathbb{Z}$ of relative dimension 1, hence projective [Liu02, Thm. 8.3.16]. In summary, we have an open immersion

$$Y \longrightarrow X$$

with X projective flat over $\mathbb{Z}$, isomorphic to X^{KM} over $\mathbb{Z}[1/p]$, regular connected of dimension 2.

Now assume that $X_{\mathbb{F}_p}$ has the smallest possible number of irreducible components. We will show that X is relatively minimal. The irreducible components of $X_{\mathbb{F}_p}$ are of two kinds: the *modular* components, which contain the image of some connected component on $Y_{\mathbb{F}_p}$, and the other components, which we call *exotic*. If $C \subset X_{\mathbb{F}_p}$ is a modular component, then the modular locus of C is an open subspace of $X_{\mathbb{F}_p}$ isomorphic as a subscheme to $\mathbb{A}^1_\kappa$ for some extension $\kappa/\mathbb{F}_p$ of degree at most two. Hence, C has multiplicity one, and C contains exactly one point outside the modular locus; moreover, an irreducible component $D \neq C \subset X_{\mathbb{F}_p}$ can only meet C at that point, since the modular locus is smooth in $X_{\mathbb{F}_p}$.

Suppose that X is not relatively minimal and let $E \subset X_{\mathbb{F}_p}$ be an exceptional divisor. Considering the contraction of E, it is clear by our assumption on X that E is a modular component with modular locus $\mathbb{A}^1_\kappa$, so $E \simeq \mathbb{P}^1_\kappa$. In particular, if $x \in E$ is the point outside the modular locus, x has residue field κ.

- Assume $p \leq 7$. Then $Y_{\mathbb{F}_p} \simeq \mathbb{A}^1_{\mathbb{F}_p}$, so there is exactly one exceptional divisor E on $X_{\mathbb{F}_p}$ which is also the only modular component, and $\kappa = \mathbb{F}_p$. Since E is exceptional, one has
$$E^2 = K_{X/\mathbb{Z}} \cdot E = -1,$$
where $K_{X/\mathbb{Z}}$ is a canonical divisor on X (cf. [Liu02, Def. 9.1.34]). For any other irreducible component D of $X_{\mathbb{F}_p}$, D is not exceptional, so $K_{X/\mathbb{Z}} \cdot D \geq 0$. This contradicts the genus formula [Liu02, Prop. 9.1.35]. Hence X is relatively minimal and it special fibre contains a component of multiplicity one; by the genus formula, $X_{\mathbb{F}_p}$ is irreducible. Since $Y(\mathbb{Q}) \neq \emptyset$, $X \to \mathrm{Spec}(\mathbb{Z})$ has geometrically integral fibres and $X_{\mathbb{Q}} \simeq \mathbb{P}^1_{\mathbb{Q}}$ by [Liu02, Prop. 7.4.1]. Therefore $X \simeq \mathbb{P}^1_{\mathbb{Z}}$ by [Liu02, Ex. 8.3.5, 8.3.6].
- Assume $p \geq 11$. Then $X^+_{\mathrm{ns}}(p)$ has genus $g \geq 1$, and its cusps are defined over $\mathbb{Q}(\zeta_p)^+$. By proposition 2.31 $Y_{\mathbb{F}_p}$ is the smooth locus of $X_{\mathbb{F}_p}$: indeed, any smooth point of $X_{\mathbb{F}_p}$ is the specialisation of a non-cuspidal point of $X(K)$ with $K/\mathbb{Q}_p$ finite unramified, hence in the image of $Y(\mathcal{O}_K)$.
In particular, every exotic component of $X_{\mathbb{F}_p}$ has multiplicity at least two. By Castelnuovo's criterion, there exists a unique component $D \subset X_{\mathbb{F}_p}$ meeting E; furthermore, D meets E transversally at x, so D is regular at x by [Liu02, Proposition 9.1.8] and D has multiplicity one. In particular, D is modular and its non-modular point is x, which is regular, so D is regular, irreducible, proper over $\mathbb{F}_p$, and its modular locus is $\mathbb{A}^1_{\kappa'}$, so $D = \mathbb{P}^1_{\kappa'}$ and $\kappa' = \kappa = \kappa(x)$.
Let $F \subset X_{\mathbb{F}_p}$ be an irreducible component distinct from E or D. Then F does not meet $(E \cup D)\backslash\{x\}$ (because it is the reunion of the modular loci of E and F), and $x \notin F$ because otherwise E would meet F, which is impossible since E is exceptional. Therefore, $E \cup D \subset X_{\mathbb{F}_p}$ is closed and open, so $X_{\mathbb{F}_p} = E \cup D$. Since E and D are regular, have multiplicity one and intersect transversally, the adjunction and genus formulae imply that $g < 1$, a contradiction.
Since $g \geq 1$, a relatively minimal model is minimal, and the formation of the regular minimal model commutes with finite étale base change or completion [Liu02, Proposition 9.3.28]. □

Remark 2.33. When $p \geq 11$, proposition 2.32 and [LT16, Theorem 1.1] imply together that the Néron model of $X^+_{\mathrm{ns}}(p)$ over $\mathbb{Z}$ is obtained by glueing $\mathscr{X}^+_{\mathrm{ns}}(p)$ and the compactification $X^{\mathrm{KM}}_{\mathbb{Z}[1/p]}$ of $\mathscr{X}^+_{\mathrm{ns}}(p)_{\mathbb{Z}[1/p]}$.

Remark 2.34. If $\mathcal{L}$ is a finite étale representable moduli problem over $\mathbb{Z}_p$, one can prove a similar minimality result for the fine moduli scheme $\mathcal{M} := \mathcal{M}(\mathcal{C}^+_{\mathrm{ns}}(p), \mathcal{L})$ when $p > 3$, if for instance $\mathcal{M}_{\mathbb{Q}_p}$ is geometrically connected and its compactification has positive genus.

When $p \leq 3$, proposition 2.31 often fails; in such cases, $\mathcal{M}$ cannot be the smooth locus of any proper regular model. Indeed, if $\mathcal{L}$ is a classical moduli problem, $\mathcal{M}$ admits K-points coming from elliptic curves with split multiplicative reduction. Such points have non-integral j-invariant, so they do not extend to $\mathcal{O}_K$.

Remark 2.35. Let $p \geq 11$. By the same proof as proposition 2.31, one can show that if $K/\mathbb{Q}_p$ is finite unramified and $n \geq 1$, the obvious map $\mathscr{X}^+_{\mathrm{ns}}(p^n)(\mathcal{O}_K) \to \mathscr{X}^+_{\mathrm{ns}}(p^n)(K)$ is also a bijection. One can then follow the proof of proposition 2.32 to show that $\mathscr{X}^+_{\mathrm{ns}}(p^n)$ identifies with the smooth non-cuspidal locus of the minimal regular model of $X^+_{\mathrm{ns}}(p^n)$.

Remark 2.36. As a consequence of this interpretation for $X^{\mathrm{sm}}_{\mathrm{EP}}(p)$, it is possible to deduce from [EP24, Corollary 3.11] a completely explicit description for the component group of the Néron model of the Jacobian of $X^+_{\mathrm{ns}}(p)$ along with its action of the Hecke algebra. Namely, this component group identifies as a module over the Hecke algebra with the quotient
$$\frac{(\mathrm{Div}(\mathcal{S}) \otimes \mathbb{Z}/(p-1)\mathbb{Z})^{\deg=0}}{\mathbb{Z}/(p-1)\mathbb{Z} \cdot u},$$
where $\mathcal{S}$ is the set of supersingular j-invariants in $\overline{\mathbb{F}_p}$, and $u = \sum_{s \in \mathcal{S}} \frac{12}{w_s}[s]$, where $2w_s$ is the size of the automorphism group of the elliptic curve with j-invariant s.

3. Arithmetic intersections on mixed Cartan curves

This section determines the arithmetic intersection number of a pair of Heegner divisors associated to coprime fundamental discriminants $\Delta_1, \Delta_2 < 0$ on the arithmetic surface of proposition 2.25

$$\mathscr{X} := \mathscr{X}^+_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}}).$$

Theorem B was stated in the introduction for $\mathscr{X}^+_{\mathrm{ns}}(p^n)$, but the arguments apply equally to arbitrary mixed Cartan curves and theorem B will be proved in that generality in § 3.4. The strategy follows Gross–Zagier [GZ85] and Gross–Kohnen–Zagier [GKZ87], reducing the intersection calculations to a counting problem for orders in quaternion algebras. We define mixed Cartan orders in § 3.2. These need not be Eichler, and we give local descriptions using the classification of Bass orders.

Notation. Let B be a quaternion algebra over $\mathbb{Q}$. We write $\mathrm{disc}(B)$ for the product of ramified primes of B. If $S \subseteq B$ is an order, we write $\mathrm{disc}(S)$ to refer to the reduced discriminant of S [Voi21, Definition 15.4.4]. The *index* of S will refer to the index $[R : S]$ of S in any maximal order $R \subseteq B$ containing S; equivalently, the index of S is equal to $\mathrm{disc}(S)/\mathrm{disc}(B)$.

3.1. Residually unramified orders.

We first recall the classification of residually unramified quaternion orders due to Brzezinski [Brz90, § 1]. For the sake of completeness, we include arguments for statements that are not immediately extracted from Brzenzinski [Brz90] or Voight [Voi21, Chapter 24].

Let S be an order in B, and for each prime p let $S_p := S \otimes \mathbb{Z}_p$. Note that $\mathbb{Z}_{p^2} := W(\mathbb{F}_{p^2})$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ are the only two unramified quadratic $\mathbb{Z}_p$-algebras up to isomorphism.

Definition 3.1. *Let $p \mid \mathrm{disc}(S)$.*

- *We say S is* residually split *at p if S_p contains a $\mathbb{Z}_p$-subalgebra $\mathcal{O} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*
- *We say S is* residually inert *at p if S_p contains a $\mathbb{Z}_p$-subalgebra $\mathcal{O} \simeq \mathbb{Z}_{p^2}$.*
- *We say S is* residually ramified *at p if every quadratic $\mathbb{Z}_p$-subalgebra of S_p is ramified over $\mathbb{Z}_p$.*

If S is either residually split or residually inert at all $p \mid \mathrm{disc}(S)$ we say S is residually unramified.

The local order S_p contains an embedding of both $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ if and only if $S_p \simeq M_2(\mathbb{Z}_p)$. So if $p \mid \mathrm{disc}(S)$ then exactly one of the three cases above must hold.

Remark 3.2. The standard definitions of residually split, inert, and ramified are expressed in terms of the isomorphism type of S_p/J_p, where J_p is the Jacobson radical of S_p; see for instance [Voi21, Definition 24.3.2]. These definitions are equivalent to those given in definition 3.1. In one direction, if S_p/J_p is isomorphic to a quadratic $\mathbb{F}_p$-algebra, let $\alpha \in S_p$ be the preimage of a generator under $S_p \to S_p/J_p$. Then $\mathbb{Z}_p[\alpha]$ is an unramified $\mathbb{Z}_p$-subalgebra of S_p, isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$ accordingly as $S_p/J_p \simeq \mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$. Conversely, for any unramified quadratic $\mathbb{Z}_p$-subalgebra $\mathcal{O} \subseteq S_p$, the map $\mathcal{O}/p\mathcal{O} \to S_p/J_p$ is an injection because $\mathcal{O}/p\mathcal{O}$ has no nonzero nilpotents.

Residually unramified orders have a simple local classification, summarised in [Voi21, § 24.5–6] for $p \neq 2$ but discussed in greater generality in [Brz90, § 1], from which the following statement may be deduced.

Lemma 3.3. *Let $p \mid \mathrm{disc}(S)$, and set $n := \mathrm{ord}_p(\mathrm{disc}(S))$. Let $\mathcal{O} \subseteq S_p$ be a quadratic $\mathbb{Z}_p$-subalgebra.*

(a) If $\mathcal{O} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ then S_p is isomorphic to an Eichler order of level p^n in $M_2(\mathbb{Z}_p)$.
(b) If $\mathcal{O} \simeq \mathbb{Z}_{p^2}$ then there is a maximal order $R_p \subseteq B_p$ such that $S_p = \mathcal{O} + p^{\lfloor n/2 \rfloor} R_p$.

Proof. Part (a) follows from [Voi21, Lemma 24.3.6], so we focus on part (b). We are done if S_p is maximal, so assume otherwise. Let R_p denote the hereditary closure of S_p, so that R_p is maximal and $p^n = \mathrm{disc}(S_p) = p^{2r}\mathrm{disc}(R_p)$ for some integer r by [Voi21, 24.4.9]. Note that S_p is Bass [Voi21, Proposition 24.5.4] and non-hereditary, so we may apply [Brz90, Proposition 1.12(a)] to write S_p as $\mathcal{O}$ plus a power of the Jacobson radical of R_p. If $R_p \simeq M_2(\mathbb{Z}_p)$ (so $n = 2r$) then the Jacobson radical of R_p is pR_p, so $S_p = \mathcal{O} + p^{n/2}R_p$. If instead R_p is the maximal order in a division algebra (so $n = 2r+1$), then its Jacobson radical is the unique maximal ideal $\mathfrak{P}$ of R_p, and we have $S_p = \mathcal{O} + \mathfrak{P}^{n-1}$. Since $\mathfrak{P}^2 = pR_p$, we may rewrite this as $S_p = \mathcal{O} + p^{(n-1)/2}R_p$. □

In what follows, we will also need the classification of superorders of residually inert orders, which follows directly from either [Voi21, Proposition 24.4.7(b)] or [Brz90, § 1].

Lemma 3.4. *Let $R_p \subseteq B_p$ be a maximal order, $\mathcal{O} \subseteq R_p$ a subalgebra with $\mathcal{O} \simeq \mathbb{Z}_{p^2}$, and $S_p = \mathcal{O} + p^k R_p$. Then every superorder $S_p' \supset S_p$ in B_p is of the form*

$$S_p' = \mathcal{O} + p^i R_p, \qquad \text{for } 0 \le i \le k.$$

3.2. **Mixed Cartan orders.** We define mixed Cartan orders in quaternion algebras over $\mathbb{Q}$. As before, we let N_{sp} and N_{ns} be a pair of coprime positive integers, and set $N := N_{\mathrm{sp}} \cdot N_{\mathrm{ns}}$.

Definition 3.5. *A* mixed Cartan order S *is a residually unramified quaternion order such that the index of S is a perfect square. The* level *of S is defined to be the positive integer N such that $[R : S] = N^2$ for any maximal order $R \supseteq S$. We say S has* type $(N_{\mathrm{sp}}, N_{\mathrm{ns}})$*, with $N_{\mathrm{sp}} \cdot N_{\mathrm{ns}} = N$, if*

- *S is residually split at every prime dividing N_{sp},*
- *S is residually inert at every prime dividing N_{ns}.*

Recall from (15) that $A(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ was defined as the unramified quadratic $(\mathbb{Z}/N\mathbb{Z})$-algebra split at primes dividing N_{sp} and inert at primes dividing N_{ns}.

Lemma 3.6. *A quaternion order S is a mixed Cartan order of type $(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ if and only if there exists a maximal order R with $NR \subset S \subset R$ and $S/NR \simeq A(N_{\mathrm{sp}}, N_{\mathrm{ns}})$. Such a maximal order R is then unique.*

Proof. Let S be mixed Cartan of type $(N_{\mathrm{sp}}, N_{\mathrm{ns}})$. For each prime p we take R_p to be the hereditary closure of S_p, which is maximal because the index of S_p in any maximal order is a square. For $p^r \parallel N_{\mathrm{ns}}$ we have $S_p \simeq \mathbb{Z}_{p^2} + p^r R_p$, so that $S_p/p^r R_p \simeq \mathbb{Z}_{p^2}/p^r\mathbb{Z}_{p^2}$, and R_p is the unique maximal order containing S_p by lemma 3.4. For $p^r \parallel N_{\mathrm{sp}}$, the Eichler order S_p is associated to a path of length $2r$ on the Bruhat–Tits tree, with each maximal superorder of S_p associated to a vertex on this path [Voi21, 23.5.16]. For $i = 0, \dots, 2r$, the inclusion of S_p into the i^{th} maximal order corresponds to the inclusion of the subring

$$\begin{pmatrix} \mathbb{Z}_p & p^i\mathbb{Z}_p \\ p^{2r-i}\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \subset M_2(\mathbb{Z}_p).$$

This subring only contains $p^r M_2(\mathbb{Z}_p)$ if $i = r$, the vertex associated to the hereditary closure. In this case it has the form $(\mathbb{Z}_p \times \mathbb{Z}_p) + p^r M_2(\mathbb{Z}_p)$, and so $S_p/p^r R_p \simeq (\mathbb{Z}/p^r\mathbb{Z})^2$. The converse is clear. □

3.3. **The Clifford order S_t.** The intersection numbers of Heegner divisors on mixed Cartan curves is encoded algebraically in the pair of embeddings of endomorphism rings

$$\mathcal{O}_1, \mathcal{O}_2 \hookrightarrow R \subset B_{q\infty} \tag{16}$$

of the associated elliptic curves, where the endomorphism ring R of their common reduction modulo q is a mixed Cartan order. We follow Gross–Kohnen–Zagier [GKZ87] and introduce the Clifford orders S_t, which are the smallest orders containing the images of a pair of embeddings as in (16). The main result of this subsection is proposition 3.9, which counts the number of mixed Cartan superorders of S_t.

Let $\Delta_1, \Delta_2 < 0$ be two negative discriminants, and let $t \in \mathbb{Z}$ satisfy $t \equiv \Delta_1\Delta_2 \bmod 2$ and $t^2 \neq \Delta_1\Delta_2$. The binary quadratic form $\Delta_1 X^2 + 2tXY + \Delta_2 Y^2$ has nonzero discriminant $4(t^2 - \Delta_1\Delta_2)$, and so its Clifford algebra over $\mathbb{Q}$ is a quaternion algebra B_t, which may be presented as

$$B_t = \mathbb{Q} + \mathbb{Q}\,e_1 + \mathbb{Q}\,e_2 + \mathbb{Q}\,e_1e_2 \qquad \text{with } \begin{cases} e_1^2 = \Delta_1,\ e_2^2 = \Delta_2 \\ e_1e_2 + e_2e_1 = 2t. \end{cases} \tag{17}$$

The integral elements $\gamma_i := (\Delta_i + e_i)/2$ generate quadratic orders $\mathcal{O}_i$ of discriminants Δ_i, where $i = 1, 2$. Their product $\gamma_1\gamma_2$ has trace $(\Delta_1\Delta_2 + t)/2$, which is an integer by our choice of t. Thus γ_1 and γ_2 generate a $\mathbb{Z}$-order S_t in the quaternion algebra B_t,

$$S_t := \mathbb{Z} + \mathbb{Z}\,\gamma_1 + \mathbb{Z}\,\gamma_2 + \mathbb{Z}\,\gamma_1\gamma_2, \qquad \text{with } \operatorname{disc}(S_t) = \frac{t^2 - \Delta_1\Delta_2}{4}. \tag{18}$$

By construction, the order S_t is generated as a ring by the image of the embeddings of the quadratic orders $\mathcal{O}_1$ and $\mathcal{O}_2$, and every such quaternion order arises in this way for an appropriate value of t.

Now suppose Δ_1, Δ_2 are coprime fundamental discriminants. As in the introduction, for any p dividing $\operatorname{disc}(S_t)$, we define $\epsilon(p)$ to be the value of the genus character χ of $\mathbb{Q}(\sqrt{\Delta_1\Delta_2})$ at any prime above p.

Lemma 3.7. *Let $\Delta_1, \Delta_2 < 0$ be a pair of coprime fundamental discriminants. Then the Clifford order S_t is residually unramified. More precisely, at any prime $p \mid \operatorname{disc}(S_t)$ we have*

- *S_t is residually split if and only if $\epsilon(p) = +1$,*
- *S_t is residually inert if and only if $\epsilon(p) = -1$.*

Proof. Since Δ_1, Δ_2 are coprime, we can pick $i = 1$ or 2 so that $\mathcal{O} := \mathcal{O}_i$ is unramified at p. Then $\mathcal{O} \otimes \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ if $\epsilon(p) = 1$, and is isomorphic to $\mathbb{Z}_{p^2}$ if instead $\epsilon(p) = -1$. □

For the proof of theorem B in the next section, we need to count the number of mixed Cartan orders of level N containing S_t. Note that $\operatorname{disc}(S_t)$ must be divisible by N^2 for this set to be non-empty.

Definition 3.8. *Given $t \in \mathbb{Z}$ with $t \equiv \Delta_1\Delta_2 \bmod 2$ and $t^2 \neq \Delta_1\Delta_2$, we define $\operatorname{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ to be the set of mixed Cartan orders R of type $(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ (cf. definition 3.5) with $S_t \subset R \subset S_t \otimes \mathbb{Q}$.*

Proposition 3.9. *Assume $\Delta_1, \Delta_2 < 0$ are two Heegner discriminants for $\operatorname{Car}(N_{\mathrm{sp}}, N_{\mathrm{ns}})$. Let S_t be the quaternion order defined by (18), and assume that $N^2 \mid \operatorname{disc}(S_t)$. Then*

$$|\operatorname{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})| = \prod_{\substack{p \mid \operatorname{disc}(S_t) \\ \epsilon(p)=1}} \left(1 + \operatorname{ord}_p\left(\frac{\Delta_1\Delta_2 - t^2}{4N^2}\right)\right)$$

Proof. It suffices to count the number of mixed Cartan superorders locally. When $p \nmid \operatorname{disc}(S_t)$ the order S_t is maximal at p, so the number is one. When $p \mid \operatorname{disc}(S_t)$ the local structure of

$$S_{t,p} := S_t \otimes \mathbb{Z}_p$$

is determined in lemma 3.3. We distinguish three cases.

- Suppose $p \mid N_{\mathrm{sp}}$. Then we must have $\epsilon(p) = +1$, so $S_{t,p}$ is an Eichler order of level p^n where $n = \mathrm{ord}_p(\mathrm{disc}(S_t))$. If $p^k \parallel N_{\mathrm{sp}}$, then locally at p, a mixed Cartan order is Eichler of level p^{2k}. Since Eichler orders of level p^n correspond to paths of length $n+1$ in the Bruhat–Tits tree [Voi21, 23.5.16], the number of Eichler orders of level p^{2k} containing an Eichler order of level p^n is
$$n + 1 - 2k = 1 + \mathrm{ord}_p(\mathrm{disc}(S_t)/N^2).$$
- Suppose $p \mid N_{\mathrm{ns}}$. Then we must have $\epsilon(p) = -1$, so writing $\mathrm{disc}(S_{t,p}) = p^n$, we can conclude that $S_{t,p} = \mathcal{O} + p^{\lfloor n/2 \rfloor} R_p$ for some maximal order R_p and quadratic subalgebra $\mathcal{O} \simeq \mathbb{Z}_{p^2}$. If $p^k \parallel N_{\mathrm{ns}}$, then $\mathcal{O} + p^k R_p$ is a mixed Cartan order of the correct type at p, and it is in fact the unique superorder of $S_{t,p}$ with the correct index, by lemma 3.4.
- Suppose $p \nmid N$. Then a mixed Cartan order of level N is maximal at p. If $\epsilon(p) = +1$ then as before the local order $S_{t,p}$ is Eichler and its number of maximal superorders equals
$$1 + \mathrm{ord}_p(\mathrm{disc}(S_t)) = 1 + \mathrm{ord}_p(\mathrm{disc}(S_t)/N^2).$$
If $\epsilon(p) = -1$ then there is a unique maximal order containing $S_{t,p}$ by lemma 3.4.

The statement of the proposition follows by taking the product of all these local counts. □

3.4. **Intersection numbers of Heegner divisors.** Let $\mathscr{X} := \mathscr{X}^+_{\mathrm{Car}}(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ as in proposition 2.25. Consider a Heegner discriminant $\Delta < 0$ for $\mathscr{X}$ as in (9), and let $\mathcal{O}$ be the quadratic order of discriminant Δ. For any invertible ideal $\mathfrak{a}$ of $\mathcal{O}$ we have a complex elliptic curve $E_{\mathfrak{a}} := \mathbb{C} \,/\, \mathfrak{a}$ with endomorphism ring $\mathcal{O}$, with a canonical injection
$$\mathcal{O}/N\mathcal{O} \hookrightarrow \mathrm{End}_{\mathbb{C}}(E_{\mathfrak{a}}[N]).$$
The ring $\mathcal{O}/N\mathcal{O}$ may be identified with the quadratic étale algebra $A := A(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ of (15). This identification is canonical up to automorphisms, giving a well-defined point $Q_{\mathfrak{a}}$ on $\mathscr{X}(\mathbb{C})$ that depends only on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O})$; we call such $Q_{\mathfrak{a}}$ a *Heegner point*. By the theory of complex multiplication, $Q_{\mathfrak{a}}$ is defined over a number field of degree $h(\mathcal{O})$ inside the ring class field of $\mathcal{O}$, and the Heegner divisor
$$P_\Delta := \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})} Q_{\mathfrak{a}} \quad \in \mathrm{Div}\ \mathscr{X}(\mathbb{Q})$$
is defined over $\mathbb{Q}$. There exists a number field L over which $E_{\mathfrak{a}}$ has all its endomorphisms defined, and has good reduction at all finite places. We obtain a point $Q_{\mathfrak{a}} \in \mathscr{X}(\mathcal{O}_L)$, and P_Δ is defined as a Cartier divisor, finite flat over $\mathbb{Z}$, so that the arithmetic intersection of two Heegner divisors on $\mathscr{X}$ is defined.

Remark 3.10. A technical complication is that the above description of the Heegner divisor uses the moduli problem $\mathcal{P}_A^+$, which is only defined over $\mathbb{Z}[1/N_{\mathrm{ns}}]$. To resolve this, note that $Q_{\mathfrak{a}} \in \mathscr{X}(L)$ comes from a $\mathcal{O}_L[1/N_{\mathrm{sp}}]$-point $C_{\mathfrak{a}}$ of $Y := \mathcal{C}^+(N_{\mathrm{sp}}, N_{\mathrm{ns}})_{E_{\mathcal{O}_L}/\mathcal{O}_L}$ using the isomorphism of corollary 2.29. Since Y is finite above $\mathcal{O}_L[1/N_{\mathrm{ns}}]$ by construction, the valuative criterion of properness ensures that $C_{\mathfrak{a}}$ extends to an $\mathcal{O}_L$-point of Y, and therefore $Q_{\mathfrak{a}}$ extends to a point in $\mathscr{X}(\mathcal{O}_L)$. Let $\mathfrak{q} \subset \mathcal{O}_L$ be a prime dividing N_{sp}, so $Q_{\mathfrak{a}}$ sends $\mathfrak{q}$ to a closed point $x \in \mathscr{X}$. There is not much one can say about the level structure determined by x, but all we will need is the fact that the underlying elliptic curve at x is the reduction of $E_{\mathfrak{a}}$ mod $\mathfrak{q}$.

Now consider a pair of Heegner points Q_1, Q_2 with Heegner discriminants $\Delta_1, \Delta_2 < 0$, and let $\mathbf{E}_1, \mathbf{E}_2$ be a pair of associated elliptic curves E_1, E_2 enriched with the Cartan-plus level structure induced by the obvious maps $\mathcal{O}_i \to \mathrm{End}(E_i[N])$. Let q be a prime, and let $\mathfrak{q}$ be a prime above q in the compositum H of the two ring class fields of discriminants Δ_1, Δ_2. By [Con04, Lemma 2.4] the points Q_1, Q_2 are defined over W, the integers of the completion of the maximal unramified extension of $H_{\mathfrak{q}}$, and we may assume that E_1, E_2 have good reduction over W with all their geometric endomorphisms defined over W. For the remainder of this section $\overline{\mathbb{F}}_q$ refers to the residue field of W (which is indeed an algebraic closure of $\mathbb{F}_q$).

Lemma 3.11. *Suppose $q \nmid N_{\mathrm{sp}}$, and that Q_1, Q_2 have the same reduction $\overline{Q}_1 = \overline{Q}_2$ in $\mathscr{X}(\overline{\mathbb{F}}_q)$. Let $x \in \operatorname{Max} \mathscr{X}_W$ be the associated closed point. Then*

$$\operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{X}_W,x}}{(Q_1,Q_2)}\right) = \frac{1}{2}\sum_{n\geq 1} |\mathrm{Isom}_{W/\mathfrak{q}^nW}(\mathbf{E}_1,\mathbf{E}_2)|. \tag{19}$$

Proof. Since $q \nmid N_{\mathrm{sp}}$, $\mathscr{X}_W$ is a smooth quotient of a smooth fine moduli space by proposition 2.25. So this follows from the arguments of Gross–Zagier [GZ86, Prop. 6.1] or Conrad [Con04, Thm. 4.1]. □

For the remainder of § 3.4 we assume that Δ_1, Δ_2 are coprime and fundamental. If the Heegner points Q_1, Q_2 have the same reduction in $\mathscr{X}(\overline{\mathbb{F}}_q)$, then using the j-invariant map $\mathscr{X} \to \mathbb{P}^1$, we can conclude $(E_1)_{\overline{\mathbb{F}}_q} \simeq (E_2)_{\overline{\mathbb{F}}_q}$. Then $\mathrm{End}_{\overline{\mathbb{F}}_q}(E_1)$ contains copies of $\mathcal{O}_1$ and $\mathcal{O}_2$, so $(E_i)_{\overline{\mathbb{F}}_q}$ is supersingular. Hence q splits in neither $\mathcal{O}_i$, and in particular $q \nmid N_{\mathrm{sp}}$. Now fix generators $u_i = (\Delta_i + \sqrt{\Delta_i})/2$ of $\mathcal{O}_i$. Let

$$j : (\mathbf{E}_1)_{\overline{\mathbb{F}}_q} \xrightarrow{\sim} (\mathbf{E}_2)_{\overline{\mathbb{F}}_q}$$

be an isomorphism of elliptic curves enriched with $\mathcal{P}_A^+$-structure. By construction, we have a ring homomorphism $\mathcal{O}_1 \otimes \mathcal{O}_2 \to W$. Using the morphisms $\mathrm{End}(E_i) \to W$ given by the Lie action, we may canonically identify $\mathcal{O}_i$ and $\mathrm{End}(E_i)$. Let $u_2' = j^{-1}u_2 j \in \mathrm{End}(E_1)$, so that

$$u_2' \in R_1 := \mathcal{O}_1 + N\mathrm{End}_{\overline{\mathbb{F}}_q}(E_1).$$

Define $t \in \mathbb{Z}$ by $\mathrm{Tr}(u_1 u_2') = (\Delta_1\Delta_2 + t)/2$. The rule $(\gamma_1, \gamma_2) \mapsto (u_1, u_2')$ defines a morphism ϕ from the Clifford order S_t of (18) to R_1. In particular, $(t^2 - \Delta_1\Delta_2)/4$ is negative and divisible by $\mathrm{disc}(R_1) = N^2 q$. Now $R := (\phi \otimes \mathbb{Q})^{-1}(R_1)$ is a mixed Cartan order in $S_t \otimes \mathbb{Q}$ of type $(N_{\mathrm{sp}}, N_{\mathrm{ns}})$, to which the maximal order attached by lemma 3.6 is

$$\mathrm{O}(R) := (\phi \otimes \mathbb{Q})^{-1}(\mathrm{End}_{\overline{\mathbb{F}}_q}(E_1)).$$

Finally, $\mathrm{O}(R)$ is oriented by the map $\omega : z \in \mathrm{O}(R) \mapsto \mathrm{Lie}(\phi(z)) \in \overline{\mathbb{F}}_q$. Thus we have defined a map

$$\Psi_W : \left\{ \left(E_1,\, E_2,\, j : (\mathbf{E}_1)_{\overline{\mathbb{F}}_q} \xrightarrow{\sim} (\mathbf{E}_2)_{\overline{\mathbb{F}}_q}\right) \right\} \longrightarrow \left\{ (t, R, \omega) : \begin{array}{l} S_t \otimes \mathbb{Q} \simeq B_{q\infty},\ \ R \in \mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}}), \\ \omega : \mathrm{O}(R) \to \overline{\mathbb{F}}_q,\ \ \omega(\gamma_i) = u_i \bmod \mathfrak{q} \end{array} \right\}, \tag{20}$$

where the E_i run over the isomorphism classes of elliptic curves over W with endomorphism ring $\mathcal{O}_i$.

Lemma 3.12. *The map Ψ_W is surjective and its fibres have cardinality $\frac{1}{2} \cdot |\,\mathcal{O}_1^\times\,| \cdot |\,\mathcal{O}_2^\times\,|$.*

Proof. Let (t, R, ω) be in the range of Ψ_W with $\omega : \mathrm{O} \to \overline{\mathbb{F}}_q$. The oriented order (O, ω) corresponds to a supersingular elliptic curve $E_0/\overline{\mathbb{F}}_q$ (cf. [Voi21, Proposition 42.4.8]). The two couples (E_i, u_i) lifting $(E_0, \phi(\gamma_i))$ are then constructed by [GZ85, Prop. 2.7].

If (E_1, E_2, j) is in the domain of Ψ_W and $\alpha_i \in \mathrm{Aut}(E_i)$, then $\Psi_W(E_1, E_2, \alpha_2 j \alpha_1) = \Psi_W(E_1, E_2, j)$. Therefore, we are reduced to showing that if $(t, R, \omega) = \Psi_W(E_1, E_2, j) = \Psi_W(E_1', E_2', j')$, there are isomorphisms $f_i : E_i \to E_i'$ such that $j' f_1 \in \mathrm{Aut}(E_2') f_2 j \mathrm{Aut}(E_1)$. Indeed, we have an isomorphism $(E_1)_{\overline{\mathbb{F}}_q} \simeq (E_1')_{\overline{\mathbb{F}}_q}$ because they have the same oriented endomorphism rings (cf. [Voi21, Prop. 42.4.8]), and the conclusion follows by using carefully the uniqueness in [GZ85, Prop 2.7]. □

Lemma 3.13. *Let $n \geq 1$. If $(t, R, \omega) = \Psi_W(E_1, E_2, j)$, then j lifts to an isomorphism $(\mathbf{E}_1)_{W/\mathfrak{q}^n} \to (\mathbf{E}_2)_{W/\mathfrak{q}^n}$ if and only if $q^{2n-1} \mid \frac{\Delta_1\Delta_2 - t^2}{4N^2}$. Such a lift is always unique.*

Proof. The uniqueness is well-known (e.g. [KM85, Th. 2.4.2]). If $q \mid \Delta_1\Delta_2$, then $(E_1)_{W/\mathfrak{q}^2} \not\simeq (E_2)_{W/\mathfrak{q}^2}$ because their q-divisible groups are not isomorphic by [Gro86, Proposition 3.3], so both conditions are equivalent to $n \leq 1$. Hence we may assume that $q \nmid \Delta_1\Delta_2$, so $\mathfrak{q}W = qW$.

Assume that j lifts to $j' : (\mathbf{E}_1)_{W/\mathfrak{q}^n} \to (\mathbf{E}_2)_{W/\mathfrak{q}^n}$. Then by Serre–Tate [KM85, Th. 2.9.1] and [Gro86, Prop. 3.3] one has

$$j^{-1}u_2 j \in \mathcal{O}_1 + N \operatorname{End}_{W/\mathfrak{q}^n W}(E_1) = \mathcal{O}_1 + Nq^{n-1} \operatorname{End}_{\overline{\mathbb{F}}_q}(E_1),$$

so

$$N^2 q^{2n-1} = \left|\operatorname{disc}\left[\mathcal{O}_1 + Nq^{n-1} \operatorname{End}_{\overline{\mathbb{F}}_q}(E_1)\right]\right| \mid |\operatorname{disc}(S_t)| = \frac{\Delta_1\Delta_2 - t^2}{4}.$$

Conversely, assume that $N^2 q^{2n-1} \mid (\Delta_1\Delta_2 - t^2)/4$. Let $R_1 = \mathcal{O}_1 + N \operatorname{End}_{\overline{\mathbb{F}}_q}(E_1)$. By considering the $\mathcal{O}_1 \otimes \mathbb{Z}_q$-module structure, one sees that

$$\phi(S_t) \otimes \mathbb{Z}_q = (\mathcal{O}_1 \otimes \mathbb{Z}_q) + q^t (R_1 \otimes \mathbb{Z}_q)$$

with $t \geq n-1$. Therefore,

$$j^{-1}u_2 j \in \mathcal{O}_1 + q^{n-1} N \operatorname{End}_{\overline{\mathbb{F}}_q}(E_1),$$

so by Serre–Tate and [Gro86, Prop. 3.3] $j^{-1}u_2 j$ lifts to some $u_2' \in \operatorname{End}_{W/\mathfrak{q}^n W}(E_1)$. By [GZ85, Prop. 2.7], $((E_1)_{W/\mathfrak{q}^n}, u_2')$ lifts to some $(E_2'/W, v_2)$ where $\operatorname{Lie}(v_2) = u_2$. Since $(E_2'/W, v_2)$ and $(E_2/W, u_2)$ are lifts of $((E_1)_{\overline{\mathbb{F}}_q}, j^{-1}u_2 j)$, they are isomorphic, so $(E_2/W, j^{-1}u_2 j)$ lifts $((E_1)_{W/\mathfrak{q}^n}, u_2')$, which implies that j lifts to $W/\mathfrak{q}^n$. □

As a corollary of the above results, we obtain the main theorem of this section, which is a generalisation of theorem B stated in the introduction to arbitrary mixed Cartan curves.

Theorem C. *Let $\Delta_1, \Delta_2 < 0$ be a pair of coprime fundamental Heegner discriminants for the mixed Cartan curve $\mathscr{X}$. Let P_1 and P_2 be their associated Heegner divisors, and $w_i := |\mathcal{O}_i^\times|$. Then*

$$\langle P_1, P_2 \rangle \;=\; \frac{w_1 w_2}{8} \cdot \sum_{\substack{t \in \mathbb{Z},\ d,d' > 0 \\ t^2 + 4N^2 dd' = \Delta_1\Delta_2}} \epsilon(d') \log(d). \tag{21}$$

Remark 3.14. The Heegner condition forces N to be coprime to $\Delta_1\Delta_2$, so if $N > 1$ then there is no contribution from $t = 0$. In this case the terms come in pairs $t, -t$ which produce the same value $m := \frac{\Delta_1\Delta_2 - t^2}{4N^2}$, from which theorem B follows. For $N = 1, t = 0$ contributes if and only if $\{\Delta_1, \Delta_2\} = \{-4, -q\}$ for an odd prime q, in which case the summand is $\log(q)$; see e.g. the first equation of [GZ85].

Proof. We first consider the left-hand side of (21), which by lemma 3.11 is

$$\sum_{q \text{ prime}} \frac{\log(q)}{2e_{W/\mathbb{Q}_q}} \sum_{E_1, E_2/W} \sum_{j : (\mathbf{E}_1)_{\overline{\mathbb{F}}_q} \xrightarrow{\sim} (\mathbf{E}_2)_{\overline{\mathbb{F}}_q}} m(j), \tag{22}$$

where $m(j)$ denotes the highest $n \geq 1$ such that j lifts to an isomorphism of enriched elliptic curves over $W/\mathfrak{q}^n$. Here, the notations $W, \mathfrak{q}$ have the same meanings as above for any given prime q. By lemmas 3.12 and 3.13, the sum (22) can be rewritten as

$$\frac{w_1 w_2}{8} \sum_{q \text{ prime}} \log(q) \sum_{\substack{t \in \mathbb{Z} \\ S_t \otimes \mathbb{Q} \simeq B_{q\infty}}} \frac{1}{e_{W/\mathbb{Q}_q}} \left(1 + \operatorname{ord}_q\left(\frac{\Delta_1\Delta_2 - t^2}{4N^2}\right)\right) |\{(R, \omega) : (t, R, \omega) \in \operatorname{im}(\Psi_W)\}|. \tag{23}$$

We next consider the right-hand side of (21). For a fixed integer t, let $m := \frac{\Delta_1\Delta_2 - t^2}{4N^2}$; note that t only contributes to the sum if m is a positive integer. As in [GZ85, p.192], one has

$$\sum_{d,d' > 0,\ dd' = m} \epsilon(d') \log(d) \;=\; \frac{1}{2} \left(\operatorname{ord}_q(m) + 1\right) \log(q) \cdot \prod_{\substack{\epsilon(p) = 1 \\ p \mid m}} \left(\operatorname{ord}_p(m) + 1\right)$$

if the set

$$\mathrm{diff}(m) := \{p \mid m \text{ prime} : \epsilon(p) = -1,\ \mathrm{ord}_p(m) = \text{ odd}\}$$

is a singleton $\{q\}$, and the sum vanishes otherwise. Now for each prime q, we have $\mathrm{diff}(m) = \{q\}$ if and only if $S_t \otimes \mathbb{Q}$ is isomorphic to the quaternion algebra $B_{q\infty}$. Therefore, by proposition 3.9, the right-hand side of (21) can be rewritten as

$$\frac{w_1 w_2}{8} \sum_{q \text{ prime}} \log(q) \sum_{\substack{t \in \mathbb{Z}, \\ S_t \otimes \mathbb{Q} \simeq B_{q\infty}}} \frac{1}{2}\left(1 + \mathrm{ord}_q\left(\frac{\Delta_1\Delta_2 - t^2}{4N^2}\right)\right) |\mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})|, \tag{24}$$

because $\mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})$ is empty if $N^2 \nmid \mathrm{disc}(S_t)$. Comparing (23) to (24), we see that the theorem holds once we can show, for each prime q and $t \in \mathbb{Z}$ with $S_t \otimes \mathbb{Q} \simeq B_{q\infty}$, that

$$\sum_{r \in \{t, -t\}} \frac{1}{e_{W/\mathbb{Q}_q}} |\{(R, \omega) : (r, R, \omega) \in \mathrm{im}(\Psi_W)\}| = \sum_{r \in \{t, -t\}} \frac{1}{2} |\mathrm{Car}_r(N_{\mathrm{sp}}, N_{\mathrm{ns}})|.$$

Assume that $q \mid \Delta_1$, so $q \nmid \Delta_2$ and $e_{W/\mathbb{Q}_q} = 2$. Let $R \in \mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})$. Let O be the maximal order associated to R by lemma 3.6. The two ring homomorphisms $\omega : \mathrm{O} \to W/\mathfrak{q}$ are conjugate under Frobenius. Both satisfy $\omega(\gamma_1) = u_1 \mod \mathfrak{q}$, and exactly one of them satisfies $\omega(\gamma_2) = u_2 \mod \mathfrak{q}$, and the conclusion follows. The same holds if $q \mid \Delta_2$.

Now assume $q \nmid \Delta_1\Delta_2$ and let $t \in \mathbb{Z}$ be such that $S_t \otimes \mathbb{Q} \simeq B_{q\infty}$. Let J_t be the set of couples (R, ω) with $R \in \mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})$, and ω is a $W/\mathfrak{q}$-valued orientation of the maximal order attached to R by lemma 3.6 sending γ_1 to $u_1 \mod \mathfrak{q}$. One has clearly $|J_t| = |\mathrm{Car}_t(N_{\mathrm{sp}}, N_{\mathrm{ns}})|$.

Let $I : S_t \to S_{-t}$ be the isomorphism respecting the first canonical generator γ_1, but sending the second canonical generator γ_2 of S_t to the quadratic conjugate of the second canonical generator of S_{-t}. Then I clearly induces a bijection $I : J_t \to J_{-t}$; furthermore, if $(R, \omega) \in J_t$ and its image under I is (R', ω'), then $(t, R, \omega) \in \mathrm{im}(\Psi_W)$ if and only if $(-t, R', \omega') \notin \mathrm{im}(\Psi_W)$. Thus one has

$$|\{(R, \omega) : (-t, R, \omega) \in \mathrm{im}(\Psi_W)\}| = |\{(R, \omega) \in J_t : (t, R, \omega) \notin \mathrm{im}(\Psi_W)\}|, \text{ hence}$$

$$\sum_{r \in \{\pm t\}} |\{(R, \omega) : (r, R, \omega) \in \mathrm{im}(\Psi_W)\}| = |J_t| = \sum_{r \in \{\pm t\}} \frac{1}{2} |\mathrm{Car}_r(N_{\mathrm{sp}}, N_{\mathrm{ns}})|,$$

and we are done. □

3.5. **Non-fundamental, non-coprime discriminants.** As was the case for counting maximal orders in Gross–Zagier [GZ85] and Eichler orders in Gross–Kohnen–Zagier [GKZ87], the assumption that Δ_1 and Δ_2 are fundamental and coprime is crucial. For maximal orders, Lauter–Viray [LV15] obtain formulae without this assumption. It is not our ambition to extend this in full to mixed Cartan orders, but we make note of a few simple generalizations here.

Proposition 3.15. *Let $\Delta_1, \Delta_2 < 0$ be coprime discriminants. Write $\Delta_1 = f_1^2 D_1$ and $\Delta_2 = f_2^2 D_2$ for fundamental discriminants D_1 and D_2. If every element of $\mathcal{S}(\Delta_1\Delta_2, N^2)$ is coprime to $f_1 f_2$, then (21) holds.*

Proof. The proof of theorem C goes through with the following modifications. By the discussion following lemma 3.11, if there is an arithmetic intersection at a prime q, then $q \mid m$ for some $m \in \mathcal{S}(\Delta_1\Delta_2, N^2)$. Hence $q \nmid f_1 f_2$, so that $e_{W/\mathbb{Q}_q} \leq 2$ (with equality iff $q \mid \Delta_1\Delta_2$). Hence [Gro86, Proposition 3.3] still applies. Moreover, in the proof that Ψ_W is onto in lemma 3.13, we need to check that the quasi-canonical lifts have CM by the order $\mathcal{O}_i$ rather than a proper super-order. This is true because, for any super-order $R \supset S_t$, the embedding $\mathcal{O}_i \hookrightarrow S_t \to R$ is optimal: indeed, it is optimal at every prime $r \nmid f_i$ because $(\mathcal{O}_i)_r$ is normal, and optimal at every prime $r \nmid |\mathrm{disc}(S_t)| \in \mathcal{S}(\Delta_1\Delta_2, N^2)$ because $\mathcal{O}_i \hookrightarrow S_t$ is optimal. □

If Δ_1 and Δ_2 are not coprime then the situation is much more subtle, but for the classification of arithmetic intersections of CM points in $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ in § 4, we can use the following weaker result. From now on we assume $p \geq 11$. By Lemma 6 and Proposition 10 of [RW25] (for $\Delta \notin \{-3,-4\}$ and $\Delta \in \{-3,-4\}$, respectively), this implies that every point in $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ with CM j-invariant is a Heegner point.

Lemma 3.16. *Let $\Delta_1, \Delta_2 < 0$ be discriminants and q a prime. Suppose $\Delta_1/\Delta_2 \neq q^{2r}$ for any $r \in \mathbb{Z}$. If their Heegner divisors on $\mathscr{X}_{\mathrm{ns}}^+(p)$ intersect at q, then $\mathcal{S}(\Delta_1\Delta_2, 1)$ contains an element divisible by p^2q.*

Proof. If P_1 and P_2 intersect at q, then as in the discussion in § 3.4, this implies that there exists an elliptic curve $E/\overline{\mathbb{F}}_q$ and injections $\mathcal{O}_1, \mathcal{O}_2 \hookrightarrow R \subseteq \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ for some mixed Cartan order R of level p. If Δ_1/Δ_2 is not a square then $\mathcal{O}_1$ and $\mathcal{O}_2$ have non-isomorphic fraction fields. If Δ_1/Δ_2 is a square, then since we are assuming Δ_1/Δ_2 is not an even power of q, there exists a prime $\ell \neq q$ such that Δ_1 and Δ_2 have distinct ℓ-adic valuations. The embeddings $\mathcal{O}_1, \mathcal{O}_2 \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ are both optimal at ℓ [LV15, Proposition 2.2], so they must land in distinct subfields.

In either case we may conclude that $\mathcal{O}_1$ and $\mathcal{O}_2$ land in distinct subfields of $B_{q\infty}$, so they generate a quaternion order of the form S_t for some value of t. Since S_t is definite, we have $t^2 < \Delta_1\Delta_2$, and since S_t is contained in a mixed Cartan order of level p in $B_{q\infty}$, we must have $qp^2 \mid \mathrm{disc}(S_t)$, so that $\mathrm{disc}(S_t)$ defines an element of $\mathcal{S}(\Delta_1\Delta_2, 1)$ divisible by p^2q. □

If $\Delta_1/\Delta_2 = q^{2r}$ for some integer r, then P_1 and P_2 can intersect at q even if $\mathcal{S}(\Delta_1\Delta_2, 1)$ has no elements divisible by p^2q. Let Δ be the "q-fundamental" discriminant dividing both Δ_1 and Δ_2 (that is, Δ_1 divided by the maximal even power of q such that the result is still a discriminant). Then by [LV15, Proposition 2.2], both embeddings $\mathcal{O}_1, \mathcal{O}_2 \to \mathrm{End}(E)$ land in an order of discriminant Δ, so it is possible that they land in the same subfield of $B_{q\infty}$. We investigate such *degenerate intersections* in the following lemma.

Lemma 3.17. *For each $i = 1, 2$, let E_i/W be an elliptic curve with CM by an order $\mathcal{O}_i$ of discriminant Δ_i in which p is inert. Let each E_i be equipped with the $\mathcal{C}_{\mathrm{ns}}^+(p)$ level structure arising from the map $\mathcal{O}_i \to \mathrm{End}(E_i[p])$. Suppose that $\Delta_1 = q^{2r}\Delta_2$ for some $r > 0$, and that $\mathcal{S}(\Delta_1\Delta_2, p^2)$ is empty. Then an isomorphism $E_1 \to E_2$ over $W/\mathfrak{q}^n$ preserves the level structures if and only if the induced isomorphism*

$$\phi : \mathrm{End}_{W/\mathfrak{q}^n}(E_1) \xrightarrow{\sim} \mathrm{End}_{W/\mathfrak{q}^n}(E_2)$$

has the property that $\phi(\mathcal{O}_1) \subset \mathcal{O}_2$.

Proof. First suppose an isomorphism $E_1 \to E_2$ over $W/\mathfrak{q}^n$ preserves the $\mathcal{C}_{\mathrm{ns}}^+(p)$ level structure. Since $\mathcal{S}(\Delta_1\Delta_2, p^2)$ is empty, there cannot exist any non-split Cartan order containing linearly independent copies of $\mathcal{O}_1$ and $\mathcal{O}_2$, so the isomorphism $\mathrm{End}_{W/\mathfrak{q}^n}(E_1) \to \mathrm{End}_{W/\mathfrak{q}^n}(E_2)$ must send $\mathcal{O}_1$ into $\mathcal{O}_2$.

Conversely, suppose we have an isomorphism over $W/\mathfrak{q}^n$ sending $\mathcal{O}_1$ into $\mathcal{O}_2$. The images of $\mathcal{O}_1$ and $\mathcal{O}_2$ in $R := \mathrm{End}_{W/\mathfrak{q}^n W}(E_2)$ generate the same subalgebra of R/pR because both conductors are coprime to p. This subalgebra determines the non-split Cartan structure on both E_1 and E_2, so the isomorphism preserves the Cartan structure. □

4. Intersections of rational CM points

Rebolledo–Wuthrich [RW25] compute with rational points on $X_{\mathrm{ns}}^+(p)$ using a moduli interpretation over $\mathbb{Z}[1/6p]$ in terms of *necklaces*, see [RW18]. As an application, they determine for $5 \leq p \leq 47$, and for any pair of Heegner discriminants of class number one

$$\Delta_1, \Delta_2 \in \{-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163\} \tag{25}$$

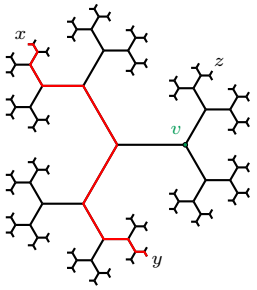
a list of primes $q \neq 2, 3, p$ for which the corresponding CM points on $X_{\mathrm{ns}}^+(p)$ have the same reduction modulo q. They expect that this is the full list of all such intersections, for any p. We confirm their results by computing the intersection multiplicities at all primes q (including $q = 2, 3, p$) of the CM points in $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ for all primes p. The "intersection numbers" $\exp(\langle P_1, P_2\rangle)$ are recorded in table 1.

4.1. **Genus zero.** For each $p = 2, 3, 5, 7$, we provide an integral model for $M \simeq \mathbb{P}^1_{\mathbb{Z}}$ for $X_{\mathrm{ns}}^+(p)$ in [Lov26]. Specificially, we provide a morphism $j : \mathbb{P}^1_{\mathbb{Z}} \to \mathbb{P}^1_{\mathbb{Z}}$ whose restriction to the generic fibre factors as an isomorphism $\phi : \mathbb{P}^1_{\mathbb{Q}} \to X_{\mathrm{ns}}^+(p)$ followed by the j-invariant map $X_{\mathrm{ns}}^+(p) \to \mathbb{P}^1_{\mathbb{Q}}$ (taken from [LMFDB]), and we use ϕ to identify the domain of j as an integral model for $X_{\mathrm{ns}}^+(p)$. The intersection numbers in table 1 were computed using this model. For each pair Δ_1, Δ_2 of coprime fundamental Heegner discriminants, these numbers — the blue entries in the table — were confirmed to agree with the predictions of theorem B (with one caveat, see remark 4.3).

Now let $\mathscr{X}_{\mathrm{ns}}^+(p) \hookrightarrow X := \mathbb{P}^1_{\mathbb{Z}}$ be an open immersion as in proposition 2.32. To show that the intersection numbers in table 1 agree with those on $\mathscr{X}_{\mathrm{ns}}^+(p)$, it suffices to confirm, for each prime q, that $M_{\mathbb{Z}_q} \simeq X_{\mathbb{Z}_q}$ as models of $X_{\mathrm{ns}}^+(p)$. We prove this by showing that both models share a certain distinguishing property.

Lemma 4.1. *Let $x, y, z \in \mathbb{P}^1(\mathbb{Q}_q)$ be distinct points, and $m \geq 0$. Then $\mathbb{P}^1_{\mathbb{Q}_q}$ has a model $M \simeq \mathbb{P}^1_{\mathbb{Z}_q}$, unique up to $\mathbb{Z}_q$-isomorphism, such that the points have intersections $\langle x, z\rangle = \langle y, z\rangle = 0$ and $\langle x, y\rangle = m$.*

Proof. The collection of isomorphism classes over $\mathbb{Z}_q$ of models $M \simeq \mathbb{P}^1_{\mathbb{Z}_q}$ is parametrized by the vertices of the $(q+1)$-regular Bruhat–Tits tree $\mathcal{T}$ whose ends are in bijection with $\mathbb{P}^1(\mathbb{Q}_q)$. Explicitly, given any such model M, every blow-up at one of its $\mathbb{F}_q$-rational points, followed by a contraction of the original special fibre, yields a neighbouring model M', see [DT08].



In the model determined by the vertex v, the intersection multiplicity of any $x, y \in \mathbb{P}^1(\mathbb{Q}_q)$ is equal to the distance of v to the path $\{x \to y\}$ in $\mathcal{T}$. So if a vertex v determines a model that satisfies the conditions of the lemma, it must lie on the paths $\{x \to z\}$ and $\{y \to z\}$, and have distance m from the path $\{x \to y\}$. There is a unique vertex v with this property. □

Given a prime q, we may use lemma 4.1 to ensure that the model M over $\mathbb{Z}_q$ used in our computations [Lov26] yields the correct intersection numbers of all CM points on $\mathscr{X}_{\mathrm{ns}}^+(p)$, by judiciously choosing a triple x, y, z and verifying that they have the correct pairwise intersection numbers on M. Let $x, y, z \in \mathscr{X}_{\mathrm{ns}}^+(p)(\mathbb{Z})$ be Heegner points with coprime fundamental discriminants that do not all intersect at q. Such a triple exists for all pairs of primes $(p, q) \neq (2, 2)$, as can be seen from the blue entries of table 1 given by theorem B. For $(p, q) = (2, 2)$, we instead take two Heegner points $x, y \in \mathscr{X}_{\mathrm{ns}}^+(2)(\mathbb{Z})$ with coprime fundamental discriminants, and $z \in X_{\mathrm{ns}}^+(2)(\mathbb{Q})$ a point with $j(z) \notin \mathbb{Z}_2$. Then the corresponding point in $X(\mathbb{Z}_2)$ does not intersect x or y.

Remark 4.2. The unusually cultured (or unusually-cultured) reader may notice that the intersection numbers on $\mathscr{X}_{\mathrm{ns}}^+(2)$ are very similar to the factorizations of differences of j-invariants: for example, compare the first equation in [GZ85] to entry $(-4, -163)$ in the $p = 2$ section of table 1. Indeed, the intersection number of P_1 and P_2 on $\mathscr{X}_{\mathrm{ns}}^+(2)$ equals the intersection number of $j(P_1)/2^{12}$ and $j(P_2)/2^{12}$ on $\mathbb{P}^1_{\mathbb{Z}}$.

Remark 4.3. There are two distinct points in $X_{\mathrm{ns}}^+(5)(\mathbb{Q})$ with CM discriminant -3, as an elliptic curve $E/\mathbb{Q}$ with j-invariant 0 can be given two non-equivalent non-split Cartan structures of level 5 over $\mathbb{Q}$.

Here is a brief explanation of the source of this extra CM point. There are 10 non-split Cartan structures on $E[5]$ over $\overline{\mathbb{Q}}$, and $\mathrm{Aut}(E)$ acts on this set. The Heegner structure, induced by the action of the CM order

$\mathrm{End}(E) = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ on $E[5]$, is naturally fixed by this action. The other nine structures come in orbits of size 3, with each orbit defining a single point of $X_{\mathrm{ns}}^+(5)(\overline{\mathbb{Q}})$. For an appropriate basis for $E[5]$, the Heegner structure $A \subset \mathrm{End}(E[5])$ can be identified with the subring of $M_2(\mathbb{F}_5)$ consisting of the elements $\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)$ for $a, b \in \mathbb{F}_5$. Now consider the subring $A_2 \subset M_2(\mathbb{F}_5)$ consisting of elements $\left(\begin{smallmatrix} a & 3b \\ b & a \end{smallmatrix}\right)$ for $a, b \in \mathbb{F}_5$. One can check that all elements of the 2-Sylow subgroup of the normalizer $N(A^\times)$ of $A^\times$ also normalize A_2, and the elements of order 3 in $A^\times$ act via $\mathrm{Aut}(E)$, so all 48 elements of $N(A^\times)$ preserve the $\mathrm{Aut}(E)$-orbit of A_2. As the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[5]$ factors through $N(A^\times)$, we can conclude that the $\mathrm{Aut}(E)$-orbit of A_2, and hence the corresponding point on $X_{\mathrm{ns}}^+(5)$, is Galois-invariant. The remaining two orbits determine a Galois-conjugate pair of points in $X_{\mathrm{ns}}^+(5)(\mathbb{Q}(\sqrt{-15}))$.

In table 1, we refer to the CM points associated to the Heegner structure A and the additional $\mathbb{Q}$-rational Cartan structure A_2 by the labels "-3" and "-3_2" respectively. Intersections involving -3_2 may not satisfy theorem B, even though the CM discriminant -3 satisfies the non-split Heegner condition for $p = 5$.

Remark 4.4. Aside from the non-Heegner CM point -3_2 on $X_{\mathrm{ns}}^+(5)$ from remark 4.3, there are also rational CM points with non-Heegner discriminant:

$$\begin{array}{rcll} \Delta & = & -4, -7, -8, -12, -16, -28 & \text{on } X_{\mathrm{ns}}^+(2), \\ \Delta & = & -3, -8, -11 & \text{on } X_{\mathrm{ns}}^+(3), \\ \Delta & = & -3 & \text{on } X_{\mathrm{ns}}^+(7). \end{array}$$

For $p \geq 11$, on the other hand, by the discussion in § 3.5, every rational CM point is a Heegner point.

4.2. **Positive genus.** From now on we assume $p \geq 11$. As Δ_1, Δ_2 range over (25), we find exactly seven triples (Δ_1, Δ_2, p) such that $\mathcal{S}(\Delta_1\Delta_2, 1)$ contains a multiple of p^2:

$$3 \cdot 11^2 \in \mathcal{S}(16 \cdot 163, 1), \quad 18 \cdot 11^2 \in \mathcal{S}(67 \cdot 163, 1), \quad 8 \cdot 11^2 \in \mathcal{S}(27 \cdot 163, 1), \quad 2 \cdot 11^2 \in \mathcal{S}(27 \cdot 67, 1),$$
$$2 \cdot 13^2 \in \mathcal{S}(11 \cdot 163, 1), \quad 12 \cdot 13^2 \in \mathcal{S}(67 \cdot 163, 1), \quad 2 \cdot 23^2 \in \mathcal{S}(27 \cdot 163, 1).$$

In each case, the multiple of p^2 in $\mathcal{S}(\Delta_1\Delta_2, 1)$ is coprime to the conductors of Δ_1 and Δ_2, so the intersection numbers of the associated Heegner points on $\mathscr{X}_{\mathrm{ns}}^+(p)$ can be computed using proposition 3.15. Alternatively, note that intersections are only possible at $q = 2, 3$ by lemma 3.16. The LMFDB [LMFDB] gives explicit models over $\mathbb{Q}$ of $X_{\mathrm{ns}}^+(p)$ for $p \in \{11, 13, 23\}$. For each pair (p, q), we use Magma to list all $\mathbb{F}_q$-points of the model for $X_{\mathrm{ns}}^+(p)$ and verify smoothness at each point. For $p \in \{11, 13\}$ we can then compute intersection multiplicities directly; for $p = 23$, we use [MS20, Table 8.3] to check that the Heegner points for discriminants -27 and -163 intersect at 2 with multiplicity 1.

Finally we consider the case that $\mathcal{S}(\Delta_1\Delta_2, 1)$ has no multiples of p^2. It follows from lemma 3.16 that an intersection of distinct Heegner points in $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ is only possible if Δ_1/Δ_2 is an even power of some prime q, in which case these points may only intersect at q. By lemma 3.11, the intersection multiplicity can be computed by counting the number of isomorphisms over $W/\mathfrak{q}^n$ that preserve the level structure. By lemma 3.17, this is equivalent to counting the number of isomorphisms over $W/\mathfrak{q}^n$ that send $\mathcal{O}_1$ into the fraction field of $\mathcal{O}_2$. Observe that this count does not depend on p: that is, if $p_0 \geq 11$ is another prime inert in the CM orders $\mathcal{O}_1$ and $\mathcal{O}_2$, and if $\mathcal{S}(\Delta_1\Delta_2, p_0^2)$ is also empty, then the intersection multiplicities at q of the Heegner points on $X_{\mathrm{ns}}^+(p)$ and $X_{\mathrm{ns}}^+(p_0)$ associated to Δ_1 and Δ_2 are equal. So for the pairs

$$(\Delta_1, \Delta_2) = (-3, -12),\ (-3, -27),\ (-4, -16),\ (-7, -28),$$

we only need to compute the intersection multiplicity at $q = 2, 3, 2$, or 2 respectively on $X_{\mathrm{ns}}^+(p_0)$ for a single prime $p_0 \geq 11$ satisfying the conditions of lemma 3.17: for $(-7, -28)$ we may take $p_0 = 13$, and for the other pairs we may take $p_0 = 11$. The intersection multiplicity equals that of the corresponding Heegner points on $X_{\mathrm{ns}}^+(p)$, for all p satisfying the same conditions. This yields the final four entries of table 1.

References

[Art86] M. Artin. "Lipman's proof of resolution of singularities for surfaces". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, New York, 1986, pp. 267–287 (↑ 14).

[BDMTV19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. "Explicit Chabauty-Kim for the split Cartan modular curve of level 13". In: *Ann. of Math. (2)* 189.3 (2019), pp. 885–944 (↑ 1).

[BDMTV23] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. "Quadratic Chabauty for modular curves: algorithms and examples". In: *Compos. Math.* 159.6 (2023), pp. 1111–1152 (↑ 1).

[BFL26] Matthew Bisatt, Lorenzo Furio, and Davide Lombardo. *Explicit p-adic Hodge theory for elliptic curves and non-split Cartan images*. Preprint, arXiv:2603.04021 [math.NT] (2026). 2026 (↑ 13).

[BP11] Y. Bilu and P. Parent. "Serre's uniformity problem in the split Cartan case". In: *Ann. of Math. (2)* 173.1 (2011), pp. 569–584 (↑ 2).

[BPR13] Y. Bilu, P. Parent, and M. Rebolledo. "Rational points on $X_0^+(p^r)$". In: *Ann. Inst. Fourier* 63.3 (2013), pp. 957–984 (↑ 2).

[Brz90] J. Brzezinski. "On automorphisms of quaternion orders". In: *J. Reine Angew. Math.* 403 (1990), pp. 166–186 (↑ 16, 17).

[Con04] B. Conrad. "Gross-Zagier revisited (with an appendix by W. R. Mann)". English. In: *Heegner points and Rankin L-series. Papers from the workshop on special values of Rankin L-series, Berkeley, CA, USA, December 2001*. Cambridge: Cambridge University Press, 2004, pp. 67–163 (↑ 19, 20).

[CSV21] Sara Chari, Daniel Smertnig, and John Voight. "On basic and Bass quaternion orders". In: *Proc. Am. Math. Soc., Ser. B* 8 (2021), pp. 11–26 (↑ 3).

[DLM22] Valerio Dose, Guido Lido, and Pietro Mercuri. "Automorphisms of Cartan modular curves of prime and composite level". In: *Algebra Number Theory* 16.6 (2022), pp. 1423–1461 (↑ 12).

[DT08] Samit Dasgupta and Jeremy Teitelbaum. "The p-adic upper half plane". In: *p-adic geometry. Lectures from the 2007 10th Arizona winter school, Tucson, AZ, USA, March 10–14, 2007*. Providence, RI: American Mathematical Society (AMS), 2008, pp. 65–121 (↑ 24).

[EL23] Bas Edixhoven and Guido Lido. "Geometric quadratic Chabauty". In: *J. Inst. Math. Jussieu* 22.1 (2023), pp. 279–333 (↑ 4).

[EP24] B. Edixhoven and P. Parent. "Regular models of modular curves in prime level over $\mathbb{Z}_p^{\mathrm{ur}}$". In: *Doc. Math.* 29.5 (2024), pp. 1017–1058 (↑ 1, 2, 13, 15).

[FL21] S. Le Fourn and P. Lemos. "Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan". In: *Algebra Number Theory* 15.3 (2021), pp. 747–771 (↑ 13).

[FL25] L. Furio and D. Lombardo. *Serre's uniformity question and proper subgroups of $C_{ns}^+(p)$*. Preprint, arXiv:2305.17780 [math.NT] (2025). 2025 (↑ 13).

[GKZ87] B. Gross, W. Kohnen, and D. Zagier. "Heegner points and derivatives of L-series. II". In: *Math. Ann.* 278.1-4 (1987), pp. 497–562 (↑ 1–3, 16, 18, 22).

[GL25] Eyal Z Goren and Jonathan Love. "Supersingular elliptic curves, quaternion algebras and applications to cryptography". In: *NATO Science for Peace and Security Series - D: Information and Communication Security*. NATO Science for Peace and Security Series D: Information and Communication Security. IOS Press, July 2025 (↑ 6).

[Gro65] A. Grothendieck. "Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Seconde partie". In: *Inst. Hautes Études Sci. Publ. Math.* 24 (1965), pp. 5–231 (↑ 14).

[Gro66] A. Grothendieck. "Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Troisième partie". In: *Inst. Hautes Études Sci. Publ. Math.* 28 (1966), pp. 5–255 (↑ 14).

[Gro67] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV". In: *Inst. Hautes Études Sci. Publ. Math.* 32 (1967), p. 361 (↑ 7).

[Gro86] B. Gross. "On canonical and quasi-canonical liftings". In: *Invent. Math.* 84 (1986), pp. 321–326 (↑ 20–22).

[GZ85] B. Gross and D. Zagier. "On singular moduli". In: *J. Reine Angew. Math.* 355 (1985), pp. 191–220 (↑ 3, 9, 16, 20–22, 24).

[GZ86] B. Gross and D. Zagier. "Heegner points and derivatives of L-series". In: *Invent. Math.* 84.2 (1986), pp. 225–320 (↑ 20).

[Hee52] Kurt Heegner. "Diophantische Analysis und Modulfunktionen". In: *Math. Z.* 56 (1952), pp. 227–253 (↑ 1, 4).

[HKLLMP] Sachi Hashimoto, Kamal Khuri-Makdisi, Guido Lido, Davide Lombardo, Nicolas Mascot, and Pierre Parent. *Equationless geometric quadratic Chabauty*. Preprint (in preparation). 2026+ (↑ 4).

[Ken85] M. A. Kenku. "A note on the integral points of a modular curve of level 7". In: *Mathematika* 32 (1985), pp. 45–48 (↑ 1).

[KM77] T. Kambayashi and M. Miyanishi. *On forms of the affine line over a field*. English. Vol. 10. Lect. Math., Dep. Math. Kyoto Univ. Kinokuniya Company Ltd., Tokyo., 1977 (↑ 11).

[KM85] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Vol. 108. Annals of Math. Studies. Princeton University Press, 1985 (↑ 2, 4, 7–14, 20, 21).

[KP16] Daniel Kohen and Ariel Pacetti. "Heegner points on Cartan non-split curves". In: *Can. J. Math.* 68.2 (2016), pp. 422–444 (↑ 4).

[Lig77] G. Ligozat. “Courbes modulaires de niveau 11”. In: *Modular functions in one variable V*. Ed. by J.-P. Serre and D. Zagier. Vol. 601. Lecture Notes in Math. Springer-Verlag, Berlin, 1977, pp. 149–237 (↑ 1).

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Erné, Oxford Science Publications. Oxford University Press, Oxford, 2002, pp. xvi+576 (↑ 14, 15).

[LLR04] Qing Liu, Dino Lorenzini, and Michel Raynaud. “Néron models, Lie algebras, and reduction of curves of genus one”. In: *Invent. Math.* 157.3 (2004). [See corrigendum in: 3858404], pp. 455–518 (↑ 5).

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database*. `https://www.lmfdb.org`. [Online; accessed 7 February 2026]. 2026 (↑ 24, 25).

[Lov26] Jonathan Love. *Non-split Cartan Intersections*. `https://github.com/jonathanrlove/nonsplit-cartan-intersections`. [Online; accessed 7 February 2026]. 2026 (↑ 24).

[LT16] Qing Liu and Jilong Tong. “Néron models of algebraic curves”. In: *Trans. Amer. Math. Soc.* 368.10 (2016), pp. 7019–7043 (↑ 15).

[LV15] Kristin Lauter and Bianca Viray. “On singular moduli for arbitrary discriminants”. In: *Int. Math. Res. Not.* 2015.19 (2015), pp. 9206–9250 (↑ 22, 23).

[Maz77] B. Mazur. “Modular curves and the Eisenstein ideal”. In: *IHÉS Publ. Math.* 47 (1977), pp. 33–186 (↑ 2).

[MS20] Pietro Mercuri and René Schoof. “Modular forms invariant under non-split Cartan subgroups”. In: *Math. Comp.* 89.324 (2020), pp. 1969–1991 (↑ 25).

[Ray74] M. Raynaud. “Schémas en groupes de type $(p, \dots, p)$”. In: *Bull. Soc. Math. France* 102 (1974), pp. 241–280 (↑ 13, 14).

[Rus70] P. Russell. “Forms of the affine line and its additive group”. In: *Pac. J. Math.* 32 (1970), pp. 527–539 (↑ 11).

[RW18] M. Rebolledo and C. Wuthrich. “A moduli interpretation for the non-split Cartan modular curve”. In: *Glasgow Math. J.* 60.2 (2018), pp. 411–434 (↑ 23).

[RW25] M. Rebolledo and C. Wuthrich. “Computing with necklaces on elliptic curves”. In: *arXiv:2509.01816* (2025) (↑ 4, 13, 23).

[Ser72] J.-P. Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”. In: *Invent. Math.* 15.4 (1972), pp. 259–331 (↑ 1, 2, 13).

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Third. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997 (↑ 1).

[SGA3I] *Schémas en groupes. I: Propriétés générales des schémas en groupes*. Vol. 151. Lecture Notes in Mathematics. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Dirigé par M. Demazure et A. Grothendieck. Springer-Verlag, Berlin-New York, 1970, pp. xv+564 (↑ 5, 8).

[Sie68] Carl Ludwig Siegel. “Zum Beweise des Starkschen Satzes”. In: *Invent. Math.* 5 (1968), pp. 180–191 (↑ 1).

[ST12] René Schoof and Nikos Tzanakis. “Integral points of a modular curve of level 11”. In: *Acta Arith.* 152.1 (2012), pp. 39–49 (↑ 1).

[Stu25] Elie Studnia. *Compactified moduli spaces and Hecke correspondences for elliptic curves with a prescribed N-torsion scheme*. 2025. arXiv: `2504.06855 [math.NT]` (↑ 5, 6, 9).

[Voi21] John Voight. *Quaternion algebras*. Vol. 288. Graduate Texts in Mathematics. Springer, Cham, 2021, pp. xxiii+885 (↑ 9, 16, 17, 19, 20).

[Zyw15] David Zywina. *On the possible images of the mod ell representations associated to elliptic curves over Q*. Preprint, arXiv: 1508.07660 [math.NT] (2015). 2015 (↑ 13).

Email address: `j.love@math.leidenuniv.nl`, Mathematical Institute, University of Leiden, 2333 CC Leiden

Email address: `e.n.g.studnia@math.leidenuniv.nl`, Mathematical Institute, University of Leiden, 2333 CC Leiden

Email address: `j.b.vonk@math.leidenuniv.nl`, Mathematical Institute, University of Leiden, 2333 CC Leiden

$p = 2$:

Δ_1, Δ_2	-4	-7	-8	-11	-12	-16	-19	-27	-28	-43	-67	-163
-3	3^3	$3^3\,5^3$	5^3	2^3	$3^3\,5^3$	$3^3\,11^3$	$2^3\,3^3$	$2^3\,3^1\,5^3$	$3^3\,5^3\,17^3$	$2^6\,3^3\,5^3$	$2^3\,3^3\,5^3\,11^3$	$2^6\,3^3\,5^3\,23^3\,29^3$
-4		$2^6\,3^6\,7^1$	$2^7\,7^2$	$7^2\,11^1$	$2^6\,3^3\,11^2$	$2^6\,3^6\,7^2$	$3^6\,19^1$	$3^1\,11^2\,23^2$	$2^6\,3^8\,7^1\,19^2$	$3^8\,7^2\,43^1$	$3^6\,7^2\,31^2\,67^1$	$3^6\,7^2\,11^2\,19^2\,127^2\,163^1$
-7			$2^6\,5^3\,7^1\,13^1$	$7^1\,13^1\,17^1\,19^1$	$2^8\,3^3\,5^3\,17^1$	$2^9\,3^7\,7^1\,19^1$	$3^7\,13^1\,31^1$	$3^1\,5^3\,17^1\,41^1\,47^1$	$2^{13}\,3^6\,5^3\,7^1\,13^1$	$3^6\,5^3\,7^1\,19^1\,73^1$	$3^7\,5^3\,7^1\,13^1\,61^1\,97^1$	$3^8\,5^3\,7^1\,13^1\,17^1\,31^1\,103^1\,229^1\,283^1$
-8			$7^2\,13^1$	$2^6\,5^3\,23^1$	$2^6\,7^2\,23^1\,31^1$	$13^1\,29^1\,37^1$	$5^3\,29^1\,53^1$	$2^6\,5^3\,7^1\,13^1\,31^1\,47^1$	$5^3\,7^2\,37^1\,61^1$	$5^4\,7^2\,13^1\,53^1\,109^1$	$5^3\,7^2\,13^1\,37^1\,101^1\,157^1\,277^1\,317^1$	
-11				$11^1\,17^1\,29^1$	$7^2\,19^1\,43^1$	$2^4\,13^1$	$2^4\,11^1\,17^1$	$7^1\,13^1\,41^1\,61^1\,73^1$	$2^3\,7^2\,19^1\,29^1$	$2^5\,7^2\,13^1\,41^1\,43^1$	$2^3\,7^2\,11^1\,13^1\,17^1\,73^1\,79^1\,107^1\,109^1$	
-12					$2^8\,3^3\,23^1\,47^1$	$3^3\,41^1\,53^1$	$3^1\,5^3\,11^2\,17^1$	$2^8\,3^3\,5^3\,59^1\,83^1$	$3^3\,5^4\,29^1\,113^1$	$3^3\,5^3\,101^1\,137^1\,197^1$	$3^8\,5^3\,11^2\,17^1\,89^1\,233^1\,293^1\,389^1$	
-16						$3^7\,67^1$	$3^1\,59^1\,83^1\,107^1$	$2^9\,3^6\,7^1\,31^1\,103^1$	$3^6\,7^2\,19^1\,163^1$	$3^8\,7^2\,11^3\,43^1$	$3^7\,7^2\,59^1\,67^1\,211^1\,571^1\,643^1$	
-19							$2^5\,3^1\,29^1$	$3^6\,13^1\,19^1\,97^1$	$2^3\,3^6\,37^1$	$2^4\,3^7\,13^1\,79^1$	$2^3\,3^7\,13^1\,19^1\,31^1\,37^1\,67^1\,193^1$	
-27								$3^1\,5^4\,89^1\,173^1$	$2^5\,3^1\,5^3\,71^1$	$2^4\,3^1\,5^3\,53^1\,113^1$	$2^3\,3^1\,5^4\,11^2\,17^1\,59^1\,137^1\,257^1$	
-28									$3^8\,5^3\,7^1\,157^1$	$3^6\,5^3\,7^1\,13^1\,41^1\,433^1$	$3^6\,5^4\,7^1\,13^1\,19^2\,73^1\,241^1\,997^1$	
-43										$2^3\,3^6\,5^3\,7^2$	$2^7\,3^6\,5^3\,7^3\,37^1\,433^1$	
-67											$2^3\,3^7\,5^3\,7^2\,13^1\,139^1\,331^1$	

$p = 3$:

Δ_1, Δ_2	-4	-7	-8	-11	-16	-19	-28	-43	-67	-163
-3	2^2	5^1	$2^2\,3^2\,5^1$	$2^5\,3^2$	$2^1\,11^1$	2^5	$5^1\,17^1$	$2^6\,5^1$	$2^5\,5^1\,11^1$	$2^6\,5^1\,23^1\,29^1$
-4		1	2^3	$2^2\,11^1$	2^1	2^2	3^2	$2^2\,3^2$	$2^2\,7^2$	$2^2\,7^2\,11^2$
-7			$5^1\,7^1$	17^1	3^1	3^1	$2^1\,5^1$	$5^1\,7^1$	$3^1\,5^1\,13^1$	$3^2\,5^1\,17^1\,31^1$
-8				$2^2\,3^3\,13^1$	$2^1\,23^1$	$2^2\,29^1$	$5^1\,47^1$	$2^2\,5^1\,7^2$	$2^2\,5^2\,53^1$	$2^2\,5^1\,101^1\,317^1$
-11					$2^1\,7^2$	2^6	$7^1\,41^1$	$2^5\,29^1$	$2^7\,41^1$	$2^5\,11^1\,17^1\,107^1$
-16						$2^1\,3^1$	7^1	$2^1\,19^1$	$2^1\,3^2\,11^1$	$2^1\,3^1\,59^1\,67^1$
-19							13^1	2^5	$2^6\,3^1$	$2^5\,3^1\,13^1\,19^1$
-28								$3^2\,5^1$	$5^1\,41^1$	$5^2\,13^1\,73^1$
-43									$2^5\,5^1$	$2^7\,5^1\,37^1$
-67										$2^5\,3^1\,5^1\,7^2$

$p = 5$:

Δ_1, Δ_2	-3_2	-7	-8	-12	-27	-28	-43	-67	-163
-3	1	1	1	2^1	3^1	1	1	2^3	2^3
-3_2		1	2^1	3^1	2^2	3^1	2^2	11^1	29^1
-7			1	1	1	2^1	3^1	3^1	$3^1\,7^1$
-8				1	2^1	1	2^1	5^1	13^1
-12					1	3^1	5^1	2^1	$2^1\,17^1$
-27						5^1	2^3	1	$5^1\,11^1$
-28							1	13^1	5^1
-43								$3^1\,7^1$	3^1
-67									$2^4\,3^2$

$p = 7$:

Δ_1, Δ_2	-4	-8	-11	-16	-43	-67	-163
-3	3^1	2^1	1	1	5^1	2^2	3^1
-4		1	1	2^1	1	1	3^2
-8			1	1	1	2^1	5^1
-11				1	2^1	1	2^2
-16					3^1	3^1	1
-43						3^1	$2^1\,7^1$
-67							13^1

$p \geq 11$ (all intersection numbers $\neq 1$):

p	11				13			23	2 mod 3	3 mod 4	3, 5, 6 mod 7
Δ_1	-16	-27	-27	-67	-11	-67		-27	-3	-4	-7
Δ_2	-163	-67	-163	-163	-163	-163		-163	-12	-16	-28
	3^1	2^1	2^2	2^1	2^1	3^1		2^1	2^1	2^1	2^1

TABLE 1. Intersection numbers $\exp(\langle P_1, P_2 \rangle)$ of CM points P_1, P_2 in $X^+_{\mathrm{ns}}(p)(\mathbb{Q})$, coloured blue when theorem B applies, green when proposition 3.15 applies (but not theorem B), and red when lemma 3.17 applies. In all other cases it is coloured black.