

MODULI SPACES OF CM ELLIPTIC CURVES AND DERIVATIVES OF EISENSTEIN SERIES

BENJAMIN HOWARD

ABSTRACT. These are notes for a six lecture mini-course at the Morningside Center of Mathematics. The goal of the lectures is to describe the calculation of the arithmetic degree of certain moduli spaces of CM elliptic curves first obtained by Kudla-Rapoport-Yang in the article “On the derivative of an Eisenstein series of weight one.”

0. INTRODUCTION

In a long series of papers Kudla [11, 12, 13, 14], Kudla-Rapoport [15, 16, 17], and Kudla-Rapoport-Yang [18, 19, 20] have given examples of relations between the geometry of some simple moduli spaces of abelian varieties with extra structure and the derivatives of Fourier coefficients of Eisenstein series. The purpose of these notes is to describe one such relation in great detail: that of [18]. This is the simplest case of those listed above, but already this example displays many of the characteristic ideas of the general program.

Briefly, the set up is as follows. Let K be a quadratic imaginary field with ring of integers \mathcal{O}_K and discriminant d_K . The nontrivial Galois automorphism of K is denoted $x \mapsto \bar{x}$. For any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ let $\mathbb{F}_{\mathfrak{p}}$ be the residue field $\mathcal{O}_K/\mathfrak{p}$. For every $m \in \mathbb{Z}^+$ there is a coarse moduli space Z_m whose points correspond to triples (E, κ, j) in which E is an elliptic curve over an \mathcal{O}_K -scheme, $\kappa : \mathcal{O}_K \rightarrow \text{End}(E)$ is an action of \mathcal{O}_K on E (a *complex multiplication*), and $j \in \text{End}(E)$ is an endomorphism of degree m which satisfies

$$\kappa(x) \circ j = j \circ \kappa(\bar{x})$$

for all $x \in \mathcal{O}_K$. Given such a triple (E, κ, j) with E defined over a field k , the subring of $\text{End}(E)$ generated by \mathcal{O}_K and j is an order in a quaternion algebra, which implies that $\text{char}(k) > 0$ and E is supersingular. The scheme Z_m is zero-dimensional and of finite type over \mathcal{O}_K , and so one may define its *arithmetic degree*

$$\text{deg}(Z_m) = \sum_{\mathfrak{p}} \log(|\mathbb{F}_{\mathfrak{p}}|) \sum_{x \in Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})} \text{length}(\mathcal{O}_{Z_m, x})$$

where the sum is over all primes \mathfrak{p} of \mathcal{O}_K . Under the additional assumption that $-d_K$ is prime, the main result of [18] is that there is a nonholomorphic modular form of weight 1

$$E^*(\tau, s) = \sum_{m=-\infty}^{\infty} a_m(v, s) \cdot e^{2\pi i m \tau}$$

(depending on a parameter $s \in \mathbb{C}$) whose functional equation

$$E^*(\tau, -s) = -E^*(\tau, s)$$

forces $E^*(\tau, 0) = 0$. Here τ lies in the upper half plane and $v = \text{Im}(\tau)$. In particular $a'_m(v, 0) = 0$. Kudla-Rapoort-Yang prove, by explicit calculation of both sides, that

$$(1) \quad \deg(Z_m) = a'_m(v, 0).$$

In these notes we will focus on the computation of the left hand side of (1). Our calculations follow broadly the methods of [18], but with some significant differences. To compute the arithmetic degree one must combine two separate calculations. First one must count the number of geometric points $|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})|$ for every prime \mathfrak{p} of \mathcal{O}_K , and then one must compute the lengths of the local rings $\text{length}(\mathcal{O}_{Z_m, x})$. The counting of geometric points is done by first proving that the cardinality $|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})|$ has a natural expression as an infinite product of local integrals, and then evaluating these local integrals. Because our arguments (unlike those of [18]) make explicit use of this product expansion, there is no need to restrict to the hypothesis that $-d_K$ is prime in the calculation of the left hand side of (1). The second calculation, the length of the local rings, is the more difficult. This calculation was originally done by Gross [5], using formal group cohomology, as one of the ingredients of the proof of the Gross-Zagier theorem [6]. This method does not generalize easily to other situations; our calculations will instead be based on Zink's theory of displays [22, 33]. In these notes we will say almost nothing about the calculation of the right hand side of (1), beyond the definition of the modular form $E^*(\tau, s)$. Of course these analytic calculations can be found in [18].

For a positive integer m let $R(m)$ denote the number of ideals $\mathfrak{m} \subset \mathcal{O}_K$ of norm m . For any prime ℓ let $R_\ell(m)$ denote the number of ideals of $\mathcal{O}_{K, \ell} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ of norm m . Thus

$$R(m) = \prod_{\ell} R_\ell(m).$$

For every prime ℓ let e_ℓ be the ramification degree of any prime of K above ℓ and let f_ℓ be the residue degree of any prime of K above ℓ . If ℓ is nonsplit in K then $e_\ell f_\ell = 2$, and if ℓ is split in K then $e_\ell f_\ell = 1$. Let $\mathbb{A}_f = \widehat{\mathbb{Q}}$ denote the ring of finite adeles of \mathbb{Q} .

1. SPECIAL ENDOMORPHISMS OF CM ELLIPTIC CURVES

1.1. A course moduli space. Suppose we are given a field F and a ring homomorphism $\mathcal{O}_K \rightarrow F$. A *CM elliptic curve* (E, κ) over F is an elliptic curve E over F together with an action $\mathcal{O}_K \rightarrow \text{End}(E)$ such that the induced action of \mathcal{O}_K on the F -vector space $\text{Lie}(E)$ is through the structure morphism $\mathcal{O}_K \rightarrow F$. More generally:

Definition 1.1.1. If S is any scheme over $\text{Spec}(\mathcal{O}_K)$ then a *CM elliptic curve* over S is a pair (E, κ) in which $E \rightarrow S$ is an elliptic curve and $\mathcal{O}_K \rightarrow \text{End}(E)$ is an action such that the induced action of \mathcal{O}_K on the \mathcal{O}_S -module $\text{Lie}(E)$ is through the structure morphism $\mathcal{O}_K \rightarrow \mathcal{O}_S$.

Remark 1.1.2. A good introduction CM elliptic curves over fields is Silverman's book [30]. A more thorough reference is Shimura's book [29]. The definitive reference for elliptic curves over general schemes is the book of Katz and Mazur [10]. Hida's book [8] is also a good resource.

We define the space of *special endomorphisms* of (E, κ)

$$L(E, \kappa) = \{j \in \text{End}(E) : \kappa(x) \circ j = j \circ \kappa(\bar{x}) \forall x \in \mathcal{O}_K\}$$

and set

$$V(E, \kappa) = L(E, \kappa) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We make $L(E, \kappa)$ into a left \mathcal{O}_K -module via the action $x \cdot j = \kappa(x) \circ j$. The \mathbb{Z} -module $L(E, \kappa)$ is equipped with a canonical quadratic form $j \mapsto \deg(j)$, and the degree satisfies

$$\deg(x \cdot j) = \text{Nm}_{K/\mathbb{Q}}(x) \cdot \deg(j)$$

for all $x \in \mathcal{O}_K$.

For any $m \in \mathbb{Z}^+$ let Z_m be the functor on the category of \mathcal{O}_K -schemes which assigns to a \mathcal{O}_K -scheme S the set $Z_m(S)$ of isomorphism classes of triples (E, κ, j) in which (E, κ) is a CM elliptic curve over S and $j \in L(E, \kappa)$ satisfies $\deg(j) = m$. The functor Z_m is not representable, but it is coarsely representable by a scheme (also denoted Z_m) of finite type over $\text{Spec}(\mathcal{O}_K)$. This can be proved using the techniques of [10] as in [18, Proposition 5.1].

Suppose that we have a CM elliptic curve (E, κ) over \mathbb{C} (after fixing a homomorphism $\mathcal{O}_K \rightarrow \mathbb{C}$). As the endomorphism ring of any elliptic curve over \mathbb{C} is either \mathbb{Z} or an order in a quadratic imaginary field, the map $\kappa : \mathcal{O}_K \rightarrow \text{End}(E)$ is an isomorphism. This clearly implies that $L(E, \kappa) = 0$. Now suppose that \mathfrak{p} is a prime ideal of \mathcal{O}_K and that we have a CM elliptic curve (E, κ) over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$. If E is ordinary then again the map $\kappa : \mathcal{O}_K \rightarrow \text{End}(E)$ is an isomorphism and so again $L(E, \kappa) = 0$. If E is supersingular then things are more interesting. In this case $\text{End}(E)$ is a maximal order in a quaternion algebra which is nonsplit exactly at p and ∞ . That is, if we set

$$H = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

then for any place $\ell \notin \{p, \infty\}$ we have $H \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \cong M_2(\mathbb{Q}_{\ell})$, while for $\ell \in \{p, \infty\}$ the ring $H \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ is the unique 4-dimensional central simple division algebra over \mathbb{Q}_{ℓ} . The Noether-Skolem theorem [4, Theorem 3.14] implies that any two embeddings of K into H are conjugate by an element of H^{\times} . In particular the embedding $x \mapsto \kappa(x)$ of K into H is conjugate to the embedding $x \mapsto \kappa(\bar{x})$, so there is a $j \in H^{\times}$ such that

$$\kappa(x) = j \cdot \kappa(\bar{x}) \cdot j^{-1}$$

for every $x \in K$. Of course, this simply says $j \in V(E, \kappa)$ and so the dimension of $V(E, \kappa)$ as a K -vector space is at least one. On the other hand the K -subspaces $\kappa(K)$ and $V(E, \kappa)$ in H intersect trivially, and it follows that

$$(2) \quad H = \kappa(K) \oplus V(E, \kappa)$$

and $\dim_K(V(E, \kappa)) = 1$. This discussion is summarized by the following proposition.

Proposition 1.1.3. *If (E, κ) is a CM elliptic curve over \mathbb{C} then $V(E, \kappa) = 0$. If (E, κ) is a CM elliptic curve over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$ then*

$$\dim_K(V(E, \kappa)) = \begin{cases} 0 & \text{if } E \text{ is ordinary} \\ 1 & \text{if } E \text{ is supersingular.} \end{cases}$$

Corollary 1.1.4. *For any $m \in \mathbb{Z}^+$ and any prime $\mathfrak{p} \subset \mathcal{O}_K$ the set $Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})$ contains only supersingular points.*

Recall the Hilbert symbol (see for example [27]): let v be a place of \mathbb{Q} and suppose $a, b \in \mathbb{Q}_v^{\times}$. We write

$$(a, b)_v = 1$$

to mean that $ax^2 + by^2 = z^2$ has a nontrivial solution with $x, y, z \in \mathbb{Q}_v$. If no nontrivial solution exists then we write $(a, b)_v = -1$. There are other useful characterizations of the Hilbert symbol. One is $(a, b)_v = 1$ if and only if a is a norm from $\mathbb{Q}_v(\sqrt{b})$. Another is $(a, b)_v = 1$ if and only there is an isomorphism

$$\left(\frac{a, b}{\mathbb{Q}_v}\right) \cong M_2(\mathbb{Q}_v).$$

Here $\left(\frac{a, b}{\mathbb{Q}_v}\right)$ is defined (see the exercises to [4, Chapter 4]) as the 4-dimensional \mathbb{Q}_v algebra generated by two elements i and j subject to the relations

$$i^2 = a \quad j^2 = b \quad ij = -ji.$$

For each $m \in \mathbb{Z}^+$ define a finite set of rational primes

$$\text{Diff}(m) = \{\ell < \infty : (-m, d_K)_\ell = -1\}.$$

Remark 1.1.5. As $(-m, d_K)_\infty = (-1, -1)_\infty = -1$ the product formula

$$\prod_{\ell \leq \infty} (-m, d_K)_\ell = 1$$

of [27, Chapter 3.2] implies that $\text{Diff}(m)$ has odd cardinality.

Remark 1.1.6. If ℓ is a rational prime which is split in K then

$$\mathbb{Q}_\ell(\sqrt{d_K}) \cong K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell.$$

Certainly this implies that $-m$ is a norm from $\mathbb{Q}_\ell(\sqrt{d_K})$, and so $(-m, d_K) = 1$. Therefore ℓ split in K implies that $\ell \notin \text{Diff}(m)$.

1.2. The counting formula of Kudla-Rapoport-Yang. The goal of these lecture notes is to prove the following theorem. Part (a) is easy. Part (b) is due (at least under the hypothesis that $-d_K$ is prime) to Kudla-Rapoport-Yang [18]. Part (c) is due to Gross [5] (see also [18, Theorem 5.11]) and was one of the essential ingredients in the proof of the Gross-Zagier theorem [6].

Theorem 1.2.1 (Kudla-Rapoport-Yang, Gross). *Suppose $m \in \mathbb{Z}^+$ and that*

$$\text{Diff}(m) = \{p\}$$

for some prime p (necessarily nonsplit in K). Let \mathfrak{p} be the unique prime of \mathcal{O}_K above p .

(a) *For every prime $\mathfrak{q} \neq \mathfrak{p}$ of \mathcal{O}_K we have*

$$Z_m(\mathbb{F}_{\mathfrak{q}}^{\text{alg}}) = \emptyset.$$

(b) *If r is the number of distinct prime factors of $-d_K$ then*

$$|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| = |\mathcal{O}_K^\times| \cdot 2^{r-1} \cdot R(mp^{e_p-2}).$$

(c) *The local ring of every point $x \in Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})$ is Artinian of length*

$$\text{length}(\mathcal{O}_{Z_m, x}) = 1 + \frac{\text{ord}_p(md_K/p)}{f_{\mathfrak{p}}}.$$

If instead $|\text{Diff}(m)| > 1$ then $Z_m = \emptyset$.

Proof. Part (a) is Corollary 1.4.2. Part (b) is Theorem 2.3.4. In Theorem 3.10.2 we will provide a complete proof of part (c) under the assumption that either (i) p is unramified in K or (ii) $p \neq 2$. We emphasize that (c) is true (and was proved by Gross) without restriction on p . The final claim is Corollary 1.4.3. \square

The *arithmetic degree* of Z_m is defined as

$$\deg(Z_m) = \sum_{\mathfrak{p}} \log(|\mathbb{F}_{\mathfrak{p}}|) \sum_{x \in Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})} \text{length}(\mathcal{O}_{Z_m, x})$$

where the sum is over all primes \mathfrak{p} of \mathcal{O}_K .

Theorem 1.2.2. *Suppose $m \in \mathbb{Z}^+$ and $\text{Diff}(m) = \{p\}$. Then*

$$\deg(Z_m) = |\mathcal{O}_K^\times| \cdot 2^{r-1} \cdot R(mp^{e_p-2}) \cdot (f_p + \text{ord}_p(md_K/p)) \cdot \log(p).$$

If $|\text{Diff}(m)| > 1$ then $\deg(Z_m) = 0$.

Proof. This is a restatement of Theorem 1.2.1. \square

1.3. Eisenstein series. Let us briefly indicate the connection between $\deg(Z_m)$ and Fourier coefficients of Eisenstein series. For the entirety of this subsection we assume that $q = -d_K$ is prime (because this hypothesis is imposed throughout [18]). For every place $\ell \leq \infty$ of \mathbb{Q} define a quadratic character $\chi_\ell : \mathbb{Q}_\ell^\times \rightarrow \{\pm 1\}$ by $\chi_\ell(x) = (x, d_K)_\ell$ and define $\chi : \mathbb{A}^\times \rightarrow \{\pm 1\}$ by

$$\chi = \prod_{\ell \leq \infty} \chi_\ell.$$

For any

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \text{SL}_2(\mathbb{Z})$$

define

$$\Phi^-(\gamma) = \begin{cases} \chi_q(a) & \text{if } q \mid c \\ iq^{-1/2} \chi_q(c) & \text{if } q \nmid c. \end{cases}$$

For $\tau = u + iv$ in the upper half complex plane and $s \in \mathbb{C}$ we set

$$(3) \quad E(\tau, s) = v^{s/2} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \frac{\Phi^-(\gamma)}{(c\tau + d)|c\tau + d|^s}$$

where $\Gamma_\infty = \{\gamma \in \Gamma \mid c = 0\}$ is the stabilizer of the cusp ∞ . If we set

$$\Lambda(s, \chi) = \pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right) L(s, \chi)$$

and define the normalized Eisenstein series

$$E^*(\tau, s) = E(\tau, s) \cdot \Lambda(s+1, \chi) \cdot q^{\frac{s+1}{2}}$$

then $E^*(\tau, s)$ satisfies the functional equation

$$-E^*(\tau, s) = E^*(\tau, -s).$$

In particular $E^*(\tau, 0) = 0$.

There is another way to define the Eisenstein series (3). For every finite place ℓ of \mathbb{Q} define a \mathbb{Q}_ℓ -quadratic space

$$(\mathcal{C}_\ell, Q_\ell) = (K_\ell, -\text{Nm}_{K/\mathbb{Q}})$$

and let $S(\mathcal{C}_\ell)$ be the space of locally constant compactly supported functions on \mathcal{C}_ℓ . Define a particular $\phi_\ell \in S(\mathcal{C}_\ell)$ by

$$\phi_\ell(x) = \mathbf{1}_{\mathcal{O}_{K,\ell}}(x).$$

At the archimedean place ∞ of \mathbb{Q} we define a real quadratic space

$$(\mathcal{C}_\infty, Q_\infty) = (K_\infty, \text{Nm}_{K/\mathbb{Q}})$$

and let $S(\mathcal{C}_\infty)$ be the space of Schwartz functions on \mathcal{C}_∞ . Define a particular $\phi_\infty \in S(\mathcal{C}_\infty)$ by

$$\phi_\infty(x) = e^{-\pi Q_\infty(x)}.$$

The collection of local quadratic spaces $\{(\mathcal{C}_\ell, Q_\ell)\}$ satisfies

$$\prod_{\ell \leq \infty} \text{hasse}_\ell(\mathcal{C}_\ell, Q_\ell) = -1,$$

and so is an *incoherent* family in the sense of Kudla.

Let $\psi : \mathbb{Q} \backslash \mathbb{A} \rightarrow \mathbb{C}^\times$ be the unramified additive character characterized by $\psi(x) = e^{2\pi i x}$ for $x \in \mathbb{R}$. For every $\ell \leq \infty$ the group $\text{SL}_2(\mathbb{Q}_\ell)$ acts on the space $S(\mathcal{C}_\ell)$ via the Weil representation ω_ψ , and we define for $g \in \text{SL}_2(\mathbb{Q}_\ell)$

$$\Phi_\ell(g) = (\omega_\psi(g)\phi_\ell)(0).$$

Every $g \in \text{SL}_2(\mathbb{Q}_\ell)$ admits an Iwasawa decomposition

$$g = \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \cdot \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \cdot k$$

with $a \in \mathbb{Q}_\ell^\times$, $b \in \mathbb{Q}_\ell$, and k an element of the maximal compact subgroup $K_\ell \subset \text{SL}_2(\mathbb{Q}_\ell)$ defined by

$$K_\ell = \begin{cases} \text{SL}_2(\mathbb{Z}_\ell) & \text{if } \ell < \infty \\ \text{SO}_2(\mathbb{R}) & \text{if } \ell = \infty. \end{cases}$$

For $s \in \mathbb{C}$ and $g \in \text{SL}_2(\mathbb{Q}_\ell)$ define

$$\Phi_\ell(g, s) = \chi_\ell(a) \cdot |a|_\ell^{s+1} \cdot \Phi_\ell(k).$$

Now for $g \in \text{SL}_2(\mathbb{A})$ set

$$\Phi(g, s) = \prod_{\ell \leq \infty} \Phi_\ell(g, s)$$

and define an adelic Eisenstein series for $g \in \text{SL}_2(\mathbb{A})$

$$\mathcal{E}(g, s) = \sum_{\gamma \in B(\mathbb{Q}) \backslash \text{SL}_2(\mathbb{Q})} \Phi(\gamma g, s)$$

where $B(\mathbb{Q}) \subset \text{SL}_2(\mathbb{Q})$ is the subgroup of upper triangular matrices. Given a $\tau = u + iv$ in the upper half plane set

$$g_\tau = \begin{pmatrix} 1 & u \\ & 1 \end{pmatrix} \cdot \begin{pmatrix} v^{1/2} & \\ & v^{-1/2} \end{pmatrix} \in \text{SL}_2(\mathbb{R}) \subset \text{SL}_2(\mathbb{A}).$$

The Eisenstein series of (3) is then equal to

$$E(\tau, s) = v^{-1/2} \mathcal{E}(g_\tau, s).$$

Kudla-Rapoport-Yang compute the Fourier expansion of $E^*(\tau, s)$, and find that

$$E^*(\tau, s) = \sum_{m=-\infty}^{\infty} a_m(v, s) \cdot e^{2\pi i m \tau}$$

in which $a_m(v, s)$ is given by the following proposition.

Proposition 1.3.1. *The constant term $a_0(v, s)$ is equal to*

$$q^{(s+1)/2} \Lambda(s+1, \chi) \cdot v^{s/2} - q^{(1-s)/2} \Lambda(1-s, \chi) \cdot v^{-s/2}.$$

If $m \neq 0$ then there is a product decomposition

$$a_m(v, s) = \prod_{\ell \leq \infty} a_{m, \ell}(v, s)$$

in which the local factors are as follows.

(a) If $\ell \neq q$ then

$$a_{m, \ell}(v, s) = \sum_{k=0}^{\text{ord}_\ell(m)} (\chi_\ell(\ell) \ell^{-s})^k.$$

(b) If $\ell = q$ then

$$a_{m, \ell}(v, s) = q^{s/2} \cdot \left(1 - \chi_q(m) q^{-s(1+\text{ord}_q(m))}\right).$$

(c) If $\ell = \infty$ then

$$a_{m, \ell}(v, s) = -\frac{2\pi^{s/2} e^{4\pi m v} v^{-s/2}}{\Gamma(s/2)} \int_{u > \max\{0, 2mv\}} e^{-2\pi u} u^{s/2} (u - 2mv)^{\frac{s}{2}-1} du.$$

Proof. See [18, §2]. □

Evaluating everything at $s = 0$ gives the following

Proposition 1.3.2. *Assume $m \neq 0$.*

(a) If $\ell < \infty$ then

$$a_{m, \ell}(v, 0) = e_\ell R_\ell(m).$$

(b) If $\ell = \infty$ then

$$a_{m, \ell}(v, 0) = \begin{cases} -2 & \text{if } m > 0 \\ 0 & \text{if } m < 0. \end{cases}$$

Proof. For $\ell < \infty$ this is an easy calculation using Proposition 1.3.1. For $\ell = \infty$ see [18, Proposition 2.6]. □

Exercise 1.3.3. Suppose $p \in \text{Diff}(m)$. Show that $a_{m, p}(v, 0) = 0$ and

$$\frac{d}{ds} a_{m, p}(v, 0) \Big|_{s=0} = e_p \log(p) R_p(mp^{e_p-2}) \cdot \frac{1 + \text{ord}_p(m)}{2}.$$

Proposition 1.3.4. *Suppose $m > 0$ and let $a'_m(v, 0)$ be the derivative of $a_m(v, 0)$ at $s = 0$. If $\text{Diff}(m) = \{p\}$ then*

$$a'_m(v, 0) = -|\mathcal{O}_K^\times| \cdot R(mp^{e_p-2}) \cdot (f_p + \text{ord}_p(md_K/p)) \cdot \log(p).$$

If $|\text{Diff}(m)| > 1$ then $a'_m(v, 0) = 0$.

Proof. Combining Proposition 1.3.2 with Exercise 1.3.3 gives

$$\begin{aligned} a'_m(v, 0) &= a'_{m, p}(v, 0) \cdot \prod_{\ell \neq p} a_{m, \ell}(v, 0) \\ &= -2 \cdot \log(p) \cdot (1 + \text{ord}_p(m)) \cdot R(mp^{e_p-2}) \\ &= -2 \cdot \log(p) \cdot (f_p + \text{ord}_p(mq/p)) \cdot R(mp^{e_p-2}) \end{aligned}$$

as desired. □

Proposition 1.3.4 implies that for $m > 0$ the central derivative $a'_m(v, 0)$ is independent of v . Combining Proposition 1.3.4 with Theorem 1.2.2 gives the following elegant result of Kudla-Rapoport-Yang (still assuming that $-d_K$ is prime): for every $m \in \mathbb{Z}^+$

$$\deg(Z_m) = -a'_m(v, 0).$$

1.4. The support of Z_m . In this subsection we will prove part (a) of Theorem 1.2.1. Fix an $m \in \mathbb{Z}^+$ and recall from Remark 1.1.6 that every prime of

$$\text{Diff}(m) = \{\ell < \infty : (d_K, -m)_\ell = -1\}$$

is nonsplit in K .

Proposition 1.4.1. *Let \mathfrak{p} be a prime of \mathcal{O}_K lying above a rational prime p . If $Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}}) \neq \emptyset$ then $\text{Diff}(m) = \{p\}$.*

Proof. Fix a point $(E, \kappa, j) \in Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})$. By Corollary 1.1.4 we know that E is a supersingular elliptic curve, and so $H = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is the rational quaternion algebra nonsplit precisely at p and ∞ . That is

$$H \otimes_{\mathbb{Q}} \mathbb{Q}_v \not\cong M_2(\mathbb{Q}_v) \iff v \in \{p, \infty\}.$$

We use the embedding $\kappa : K \rightarrow H$ to view K as a subalgebra of H . Consider $j + j^\vee \in H$. On the one hand $j + j^\vee \in \mathbb{Z}$ (any endomorphism of E which is self-dual is multiplication by an integer). On the other hand for any $x \in K$ we have

$$\begin{aligned} x(j + j^\vee) &= xj + xj^\vee \\ &= xj + (\bar{x})^\vee j^\vee \\ &= xj + (j\bar{x})^\vee \\ &= j\bar{x} + (xj)^\vee \\ &= j\bar{x} + j^\vee \bar{x} \\ &= (j + j^\vee)\bar{x}. \end{aligned}$$

But we already said that $j + j^\vee \in \mathbb{Z}$ so commutes with every $x \in K$. We deduce that $j + j^\vee = 0$. In particular

$$m = \deg(j) = j \circ j^\vee = -j^2.$$

If we set $\delta = \sqrt{-d_K} \in K \subset H$ then we find that the \mathbb{Q} -algebra H is generated by two elements δ, j which satisfy the relations

$$\delta^2 = d_K \quad j^2 = -m \quad \delta j = -j\delta$$

and so there is an isomorphism of quaternion algebras

$$H \cong \left(\frac{d_K, -m}{\mathbb{Q}} \right).$$

But we know that H is nonsplit precisely at p and ∞ , and so for every place $\ell \leq \infty$ of \mathbb{Q}

$$(d_K, -m)_\ell = \begin{cases} 1 & \text{if } \ell \neq p, \infty \\ -1 & \text{if } \ell = p, \infty. \end{cases}$$

In other words $\text{Diff}(m) = \{p\}$. □

Corollary 1.4.2. *If $\text{Diff}(m) = \{p\}$ then there is a unique prime $\mathfrak{p} \subset \mathcal{O}_K$ above p , and $Z_m(\mathbb{F}_{\mathfrak{q}}^{\text{alg}}) = \emptyset$ for every prime $\mathfrak{q} \neq \mathfrak{p}$.*

Proof. If $Z_m(\mathbb{F}_q^{\text{alg}}) \neq \emptyset$ then the proposition shows that $\text{Diff}(m) = \{q\}$ where $q = \mathfrak{q} \cap \mathbb{Z}$. Therefore $p = q$, and as both p and q are nonsplit in K we must have $\mathfrak{p} = \mathfrak{q}$. \square

Corollary 1.4.3. *If $|\text{Diff}(m)| > 1$ then $Z_m = \emptyset$.*

Proof. As Z_m is of finite type over $\text{Spec}(\mathcal{O}_K)$, if Z_m is not the empty scheme then there is some prime \mathfrak{p} of \mathcal{O}_K for which $Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}}) \neq \emptyset$. But of course the proposition then implies that $|\text{Diff}(m)| = 1$. \square

2. COUNTING GEOMETRIC POINTS

In this section we will prove part (b) of Theorem 1.2.1. The method of proof is not essentially different from the method used in [18], but our proof will exploit a feature which is never explicitly stated in [18]. Namely that the cardinality $|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})|$ has a natural factorization as a product of local factors. Thus our proof of Theorem 1.2.1 part (b) will proceed in two steps: first the existence of a factorization

$$|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| = \frac{|\mathcal{O}_K^\times|}{2} \cdot \prod_{\ell} O_{\ell}(E, \kappa, m).$$

in which each $O_{\ell}(E, \kappa, m)$ is local *orbital integral*, and then the calculation of the orbital integral for every prime ℓ .

2.1. Class groups and algebraic groups. Let $\text{Pic}(\mathcal{O}_K)$ be the ideal class group of K . Fix an embedding $K \rightarrow \mathbb{C}$ and suppose that (E, κ) is a CM elliptic curve over \mathbb{C} . Then there is an \mathcal{O}_K -stable lattice $\Lambda \subset \mathbb{C}$ and an \mathcal{O}_K -linear isomorphism of complex tori

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

If \mathfrak{a} is any fractional \mathcal{O}_K -ideal then there is an isomorphism of groups

$$\mathfrak{a} \otimes_{\mathcal{O}_K} (\mathbb{C}/\Lambda) \cong \mathbb{C}/\mathfrak{a}\Lambda$$

defined by $a \otimes z \mapsto az$. If we denote by $\mathfrak{a} \otimes E$ the elliptic curve over \mathbb{C} whose complex points are $\mathbb{C}/\mathfrak{a}\Lambda$ then the above isomorphism reads

$$\mathfrak{a} \otimes_{\mathcal{O}_K} E(\mathbb{C}) \cong (\mathfrak{a} \otimes E)(\mathbb{C}).$$

In this way the group $\text{Pic}(\mathcal{O}_K)$ acts on the set of all (isomorphism classes of) CM elliptic curves over \mathbb{C} .

Exercise 2.1.1. Prove that the action of $\text{Pic}(\mathcal{O}_K)$ on the set of isomorphism classes of CM elliptic curves over \mathbb{C} is simply transitive.

Now suppose (E, κ) is a CM elliptic curve over any \mathcal{O}_K -scheme S and \mathfrak{a} is a fractional \mathcal{O}_K -ideal. We define a functor from the category of S -schemes to the category of \mathcal{O}_K -modules by

$$T \mapsto \mathfrak{a} \otimes_{\mathcal{O}_K} E(T).$$

A fundamental fact, due to Serre and described in [1, §7], is that this functor is represented by an elliptic curve over S which we denote by $\mathfrak{a} \otimes E$. In other words $\mathfrak{a} \otimes E$ is defined by the relation

$$(\mathfrak{a} \otimes E)(T) \cong \mathfrak{a} \otimes_{\mathcal{O}_K} E(T)$$

for every scheme $T \rightarrow S$. As \mathcal{O}_K naturally acts on $\mathfrak{a} \otimes E$ we obtain a new CM elliptic curve over S

$$\mathfrak{a} \otimes (E, \kappa) = (\mathfrak{a} \otimes E, \kappa).$$

The isomorphism class of $\mathfrak{a} \otimes (E, \kappa)$ depends only on the image of \mathfrak{a} in $\text{Pic}(\mathcal{O}_K)$, and so for any scheme the above construction defines an action of $\text{Pic}(\mathcal{O}_K)$ on the set of isomorphism classes of CM elliptic curves over S .

Let T and T^1 be the algebraic groups over \mathbb{Q} whose functors of points are given by

$$\begin{aligned} T(A) &= (K \otimes_{\mathbb{Q}} A)^{\times} \\ T^1(A) &= \{x \in T(A) : x\bar{x} = 1\} \end{aligned}$$

for any \mathbb{Q} -algebra A . In particular $T(\mathbb{A}_f) = \widehat{K}^{\times}$ and $T^1(\mathbb{A}_f) \subset T(\mathbb{A}_f)$ is the subgroup of elements of norm 1. Define

$$U = \widehat{\mathcal{O}}_K^{\times} \subset T(\mathbb{A}_f)$$

and note that there is an isomorphism

$$T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U \cong \text{Pic}(\mathcal{O}_K)$$

defined by $t \mapsto \mathfrak{a}$, where \mathfrak{a} is the fractional \mathcal{O}_K -ideal defined by $t\widehat{\mathcal{O}}_K = \mathfrak{a}\widehat{\mathcal{O}}_K$.

Exercise 2.1.2. Define a homomorphism

$$\rho : T \rightarrow T^1$$

by $\rho(x) = x/\bar{x}$. Prove that if k is a field of characteristic 0 then the sequence

$$1 \rightarrow k^{\times} \rightarrow T(k) \rightarrow T^1(k) \rightarrow 1$$

is exact (hint: first assume that k is algebraically closed, then use Hilbert's theorem 90 for the general case).

Exercise 2.1.3. Repeat the previous exercise with $k = \mathbb{A}_f$ (hint: see [23, Corollary 8.1.1] for the adelic version of Hilbert's Theorem 90). Deduce that ρ induces an isomorphism of groups

$$(4) \quad T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U \cong T^1(\mathbb{Q}) \backslash T^1(\mathbb{A}_f) / \rho(U).$$

Fix a prime p which is nonsplit in K and let \mathfrak{p} be the prime of \mathcal{O}_K above p . Let (E, κ) be a supersingular CM elliptic curve over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$, and recall that K acts on $V(E, \kappa)$ by $x \cdot j = \kappa(x) \circ j$. Restricting this action to $T^1(\mathbb{Q}) \subset K^{\times}$ gives an action of $T^1(\mathbb{Q})$ which identifies $T^1(\mathbb{Q})$ with the special orthogonal group of $V(E, \kappa)$. In particular the stabilizer in $T^1(\mathbb{Q})$ of any nonzero vector is trivial, and for any $m \in \mathbb{Q}^{\times}$ the set

$$\{j \in V(E, \kappa) : \deg(j) = m\}$$

is either empty or is a simply transitive $T^1(\mathbb{Q})$ -set. Define an action of $T(\mathbb{Q})$ on $V(E, \kappa)$ by

$$t \bullet j = \rho(t) \cdot j = \kappa(t) \circ j \circ \kappa(t)^{-1}.$$

2.2. Reduction to orbital integrals. Let p be a prime which is nonsplit in K and let \mathfrak{p} be the prime of K above p . Fix an $m \in \mathbb{Z}^+$ and let $Z(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})$ be the set of isomorphism classes of CM elliptic curves over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$, so that

$$(5) \quad |Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| = \sum_{(E, \kappa) \in Z(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})} \sum_{\substack{j \in V(E, \kappa) \\ \deg(j) = m}} \mathbf{1}_{\widehat{L}(E, \kappa)}(j)$$

where $\mathbf{1}_{\widehat{L}(E, \kappa)}$ is the characteristic function of $\widehat{L}(E, \kappa) \subset \widehat{V}(E, \kappa)$. By fixing one CM elliptic curve (E, κ) over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$ and using the fact that

$$\text{Pic}(\mathcal{O}_K) \cong T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U$$

acts simply transitively on the set of all CM elliptic curves (see Corollary 3.7.7) we may rewrite (5) as

$$(6) \quad |Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| = \sum_{\mathfrak{a} \in \text{Pic}(\mathcal{O}_K)} \sum_{\substack{j \in V(\mathfrak{a} \otimes E, \kappa) \\ \deg(j) = m}} \mathbf{1}_{\widehat{L}(\mathfrak{a} \otimes E, \kappa)}(j).$$

In the inner sum $t \in T(\mathbb{A}_f)$ and $\mathfrak{a} \subset K$ are related by $t\widehat{\mathcal{O}}_K = \mathfrak{a}\widehat{\mathcal{O}}_K$.

For every fractional \mathcal{O}_K -ideal \mathfrak{a} there is a natural \mathcal{O}_K -linear quasi-isogeny

$$f : E \rightarrow \mathfrak{a} \otimes E$$

given on points by $P \mapsto 1 \otimes P$, and this quasi-isogeny induces an isomorphism

$$(7) \quad \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \text{End}(\mathfrak{a} \otimes E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

defined by $j \mapsto f \circ j \circ f^{-1}$.

Exercise 2.2.1. Deduce from [1, Lemma 7.14] that the isomorphism (7) carries the \mathcal{O}_K -submodule

$$\kappa(\mathfrak{a}) \circ \text{End}(E) \circ \kappa(\mathfrak{a}^{-1}) \subset \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

isomorphically to $\text{End}(\mathfrak{a} \otimes E)$, and carries

$$\kappa(\mathfrak{a}) \circ L(E, \kappa) \circ \kappa(\mathfrak{a}^{-1})$$

isomorphically to $L(\mathfrak{a} \otimes E, \kappa)$.

If $t \in T(\mathbb{A}_f)$ satisfies $t\widehat{\mathcal{O}}_K = \mathfrak{a}\widehat{\mathcal{O}}_K$ then the above lemma may be rewritten as

$$\begin{aligned} \widehat{L}(\mathfrak{a} \otimes E, \kappa) &= \kappa(t) \circ \widehat{L}(E, \kappa) \circ \kappa(t)^{-1} \\ &= t \bullet \widehat{L}(E, \kappa) \end{aligned}$$

as $\widehat{\mathcal{O}}_K$ -lattices in $\widehat{V}(E, \kappa)$. We now rewrite (6) as

$$\begin{aligned} |Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| &= \sum_{t \in T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U} \sum_{\substack{j \in V(E, \kappa) \\ \deg(j) = m}} \mathbf{1}_{t \bullet \widehat{L}(E, \kappa)}(j) \\ &= \sum_{t \in T^1(\mathbb{Q}) \backslash T^1(\mathbb{A}_f) / \rho(U)} \sum_{\substack{j \in V(E, \kappa) \\ \deg(j) = m}} \mathbf{1}_{t \bullet \widehat{L}(E, \kappa)}(j) \end{aligned}$$

where the second equality follows by replacing t by $\rho(t)$ and using (4). If $V(E, \kappa)$ does not represent m then clearly $|Z_m(\mathbb{F}_{\mathfrak{p}}^{\text{alg}})| = 0$. Suppose then that there is some

$j \in V(E, \kappa)$ such that $\deg(j) = m$. As noted earlier, the action of $T^1(\mathbb{Q})$ on the set of all such j is simply transitive, and if we fix one such j then

$$\begin{aligned} |Z_m(\mathbb{F}_p^{\text{alg}})| &= \sum_{t \in T^1(\mathbb{Q}) \backslash T^1(\mathbb{A}_f) / \rho(U)} \sum_{\gamma \in T^1(\mathbb{Q})} \mathbf{1}_{t \cdot \widehat{L}(E, \kappa)}(\gamma^{-1} \cdot j) \\ &= \sum_{t \in T^1(\mathbb{Q}) \backslash T^1(\mathbb{A}_f) / \rho(U)} \sum_{\gamma \in T^1(\mathbb{Q})} \mathbf{1}_{\gamma t \cdot \widehat{L}(E, \kappa)}(j) \\ &= |T^1(\mathbb{Q}) \cap \rho(U)| \cdot \sum_{t \in T^1(\mathbb{A}_f) / \rho(U)} \mathbf{1}_{t \cdot \widehat{L}(E, \kappa)}(j). \end{aligned}$$

One checks that

$$T^1(\mathbb{Q}) \cap \rho(U) \cong (T(\mathbb{Q}) \cap U) / \{\pm 1\} = \mathcal{O}_K^\times / \{\pm 1\}$$

leaving us with

$$(8) \quad |Z_m(\mathbb{F}_p^{\text{alg}})| = \frac{|\mathcal{O}_K^\times|}{2} \cdot \sum_{t \in T^1(\mathbb{A}_f) / \rho(U)} \mathbf{1}_{t \cdot \widehat{L}(E, \kappa)}(j).$$

For any prime ℓ abbreviate

$$L_\ell(E, \kappa) = L(E, \kappa) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad V_\ell(E, \kappa) = V(E, \kappa) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Definition 2.2.2. Suppose (E, κ) is a CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$. For any prime ℓ define the *local orbital integral*

$$O_\ell(E, \kappa, m) = \sum_{t \in T^1(\mathbb{Q}_\ell) / \rho(U_\ell)} \mathbf{1}_{L_\ell(E, \kappa)}(t^{-1} \cdot j)$$

where $j \in V_\ell(E, \kappa)$ satisfies $\deg(j) = m$. If no such j exists then set $O_\ell(E, \kappa, m) = 0$. As the action of $T^1(\mathbb{Q}_\ell)$ is transitive on the set of all such j this definition does not depend on the choice of j .

Proposition 2.2.3. *If (E, κ) is any CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$ and $m \in \mathbb{Z}^+$ then*

$$|Z_m(\mathbb{F}_p^{\text{alg}})| = \frac{|\mathcal{O}_K^\times|}{2} \cdot \prod_{\ell} O_\ell(E, \kappa, m).$$

Proof. If $V(E, \kappa)$ does not represent m then by the Hasse-Minkowski theorem there is a place $\ell \leq \infty$ of \mathbb{Q} such that $V_\ell(E, \kappa)$ does not represent m . As \deg is positive definite and $m > 0$, certainly $V_\infty(E, \kappa)$ represents m . Therefore there is some prime $\ell < \infty$ for which $V_\ell(E, \kappa)$ does not represent m . This implies that $O_\ell(E, \kappa, m) = 0$ and so both sides of the stated equality are 0. If $V(E, \kappa)$ does represent m then the desired equality is just a restatement of (8). \square

2.3. Calculation of orbital integrals. Let m be a positive integer. Fix a prime p which is nonsplit in K and let \mathfrak{p} be the prime of K above p . Let (E, κ) be a supersingular CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$.

Proposition 2.3.1. *Suppose $\ell \neq p$. There is an $\mathcal{O}_{K, \ell}$ -linear isomorphism of quadratic spaces*

$$(\mathcal{O}_{K, \ell}, -\text{Nm}_{K/\mathbb{Q}}) \cong (L_\ell(E, \kappa), \deg).$$

Proof. The ℓ -adic Tate module $T_\ell = \text{Ta}_\ell(E)$ is free of rank one over $\mathcal{O}_{K,\ell}$. If we fix an isomorphism of $\mathcal{O}_{K,\ell}$ -modules $T_\ell \cong \mathcal{O}_{K,\ell}$ then

$$\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \text{End}_{\mathbb{Z}_\ell}(T_\ell) \cong \text{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell}).$$

If we let $j_0 \in \text{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell})$ be defined by $j_0(x) = \bar{x}$ then

$$\text{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell}) = \mathcal{O}_{K,\ell} \oplus \mathcal{O}_{K,\ell} \cdot j_0$$

and $L_\ell(E, \kappa) = \mathcal{O}_{K,\ell} \cdot j_0$. For any $xj_0 \in L_\ell(E, \kappa)$ we have

$$\deg(xj_0) = -(xj_0)^2 = -x\bar{x}j_0^2 = -\text{Nm}_{K/\mathbb{Q}}(x)$$

where the second equality follows from the proof of Proposition 1.4.1. Thus $x \mapsto xj$ provides the desired isomorphism. \square

Proposition 2.3.2. *There is an $\mathcal{O}_{K,p}$ -linear isomorphism of quadratic spaces*

$$(9) \quad (\mathcal{O}_{K,p}, \beta_p \cdot \text{Nm}) \cong (L_p(E, \kappa), \deg)$$

for some $\beta_p \in \mathbb{Z}_p$ satisfying

$$\text{ord}_p(\beta_p) = 2 - e_p.$$

Proof. Set $H = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ and use $\kappa : \mathcal{O}_K \rightarrow \text{End}(E)$ to view K as a subalgebra of H . By the discussion surrounding (2) there is a decomposition of K_p -vector spaces

$$H_p = K_p \oplus K_p \cdot j$$

for any $j \in V_p(E, \kappa)$. If we choose j to be a $\mathcal{O}_{K,p}$ -generator of $L_p(E, \kappa)$ then $x \mapsto xj$ defines an isomorphism of quadratic spaces (9) with $\beta_p = j^2 = -\deg(j)$. As there is an isomorphism of quaternion algebras

$$H_p \cong \left(\frac{d_K, \beta_p}{\mathbb{Q}_p} \right)$$

we must have $(d_K, \beta_p)_p = -1$.

In order to determine $\text{ord}_p(\beta_p)$ we exploit the fact that $\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the unique maximal order in H_p , and is the valuation ring of the discrete valuation \deg . In other words $j \in H_p$ lies in $\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ if and only if $\deg(j) \in \mathbb{Z}_p$. Suppose first that p is unramified in K . The condition $(d_K, \beta_p)_p = -1$ is equivalent to $\text{ord}_p(\beta_p) \equiv 1 \pmod{2}$. If $\text{ord}_p(\beta_p) \geq 3$ then $\deg(j/p) \in \mathbb{Z}_p$, and so $j/p \in L_p(E, \kappa)$. This contradicts j generating $L_p(E, \kappa)$ as an $\mathcal{O}_{K,p}$ -module, and so we must have $\text{ord}_p(\beta_p) = 1$. Now suppose that p is ramified in K and let $\varpi \in \mathcal{O}_{K,p}$ be a uniformizing parameter. If $\text{ord}_p(\beta_p) > 0$ then $\deg(\varpi^{-1}j) \in \mathbb{Z}_p$, and so $\varpi^{-1}j \in L_p(E, \kappa)$. Again this contradicts j generating $L_p(E, \kappa)$ as an $\mathcal{O}_{K,p}$ -module, and so we must have $\text{ord}_p(\beta_p) = 0$. \square

Proposition 2.3.3. *Let ℓ be any prime. If the quadratic space $V_\ell(E, \kappa)$ represents m then*

$$\mathcal{O}_\ell(E, \kappa, m) = e_\ell R_\ell(m p^{e_p - 2}).$$

Proof. Fix a $j \in V_\ell(E, \kappa)$ such that $\deg(j) = m$. We identify $L_\ell(E, \kappa) \cong \mathcal{O}_{K,\ell}$ as in Propositions 2.3.1 and 2.3.2. Thus $m\beta_\ell^{-1} = \text{Nm}_{K/\mathbb{Q}}(j)$ where $\beta_\ell = -1$ if $\ell \neq p$, and β_p is as in Proposition 2.3.2. We must find a set of coset representatives $S \subset T^1(\mathbb{Q}_\ell)$ for

$$(10) \quad \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell) / U_\ell \cong T^1(\mathbb{Q}_\ell) / \rho(U_\ell)$$

and compute

$$O_\ell(E, \kappa, m) = \sum_{s \in S} \mathbf{1}_{\mathcal{O}_{K,\ell}}(s^{-1} \cdot j).$$

Suppose first that ℓ is inert in K . Then $\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{1\}$ gives a complete set of coset representatives for the left hand side of (10), and applying ρ gives the coset representatives $\{1\}$ for the right hand side of (10). We now see from $\text{Nm}_{K/\mathbb{Q}}(j) \in \mathbb{Z}_\ell$ that

$$O_\ell(E, \kappa, m) = \mathbf{1}_{\mathcal{O}_{K,\ell}}(j) = R_\ell(m\beta_\ell^{-1}).$$

Suppose next that ℓ is ramified in K and let $\varpi \in \mathcal{O}_{K,\ell}$ be a uniformizing parameter. Then $\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{1, \varpi\}$ gives a complete set of coset representatives for the left hand side of (10), and applying ρ gives the coset representatives $\{1, u\}$ for the right hand side of (10), where $u = \varpi/\overline{\varpi} \in \mathcal{O}_{K,\ell}^\times$. Again using $\text{Nm}_{K/\mathbb{Q}}(j) \in \mathbb{Z}_\ell$ we see that

$$O_\ell(E, \kappa, m) = \mathbf{1}_{\mathcal{O}_{K,\ell}}(j) + \mathbf{1}_{\mathcal{O}_{K,\ell}}(u \cdot j) = 2 \cdot R_\ell(m\beta_\ell^{-1}).$$

Finally suppose that ℓ is split in K and fix an isomorphism $K_\ell \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell$. Then

$$\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{(\ell^k, 0) : k \in \mathbb{Z}\}$$

gives a complete set of coset representatives for the left hand side of (10), and applying ρ gives the coset representatives $\{(\ell^k, \ell^{-k}) : k \in \mathbb{Z}\}$ for the right hand side of (10). In this case, writing $j = (j_1, j_2) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ we find

$$\begin{aligned} O_\ell(E, \kappa, m) &= \sum_{k=-\infty}^{\infty} \mathbf{1}_{\mathbb{Z}_\ell \times \mathbb{Z}_\ell}(\ell^k j_1, \ell^{-k} j_2) \\ &= 1 + \text{ord}_\ell(j_1) + \text{ord}_\ell(j_2) \\ &= 1 + \text{ord}_\ell(m\beta_\ell^{-1}) \\ &= R_\ell(m\beta_\ell^{-1}). \end{aligned}$$

□

Theorem 2.3.4. *If $\text{Diff}(m) = \{p\}$ then*

$$|Z_m(\mathbb{F}_p^{\text{alg}})| = |\mathcal{O}_K^\times| \cdot 2^{r-1} \cdot R(mp^{e_p-2})$$

where r is the number of distinct prime divisors of d_K .

Proof. Let E be a supersingular CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$, so that $H = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion division algebra nonsplit precisely at p and ∞ . The condition $\text{Diff}(m) = \{p\}$ is equivalent to

$$(d_K, -m)_\ell = \begin{cases} 1 & \text{if } \ell \neq p, \infty \\ -1 & \text{if } \ell = p, \infty \end{cases}$$

and so there is an isomorphism

$$H \cong \left(\frac{d_K, -m}{\mathbb{Q}} \right).$$

Choose elements $\delta, j \in H$ satisfying

$$\delta^2 = d_K \quad j^2 = -m \quad \delta j = -j\delta.$$

We now embed $K \rightarrow H$ by $\sqrt{d_K} \mapsto \delta$. It may not be the case that $\mathcal{O}_K[j] \subset \text{End}(E)$, but $\text{End}(E)$ is a maximal order in H and $\mathcal{O}_K[j]$ is contained in *some* maximal order $\mathcal{O}_H \subset H$ [32, Proposition I.4.2]. Replacing E by an isogenous elliptic curve we may

then assume that $\mathcal{O}_H = \text{End}(E)$ (see exercise 2.3.5 below). We therefore obtain a supersingular elliptic curve (E, κ) and a $j \in V(E, \kappa)$ satisfying $\deg(j) = m$. Proposition 2.2.3 asserts that

$$|Z_m(\mathbb{F}_p^{\text{alg}})| = \frac{|\mathcal{O}_K^\times|}{2} \cdot \prod_{\ell} O_{\ell}(E, \kappa, m)$$

and so the claim follows from Proposition 2.3.3. \square

Exercise 2.3.5. Let E be a supersingular elliptic curve over $\mathbb{F}_p^{\text{alg}}$ and set $H = \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. If $\mathcal{O}_H \subset H$ is any maximal order, show that there is an elliptic curve E' over $\mathbb{F}_p^{\text{alg}}$ which is isogenous to E and satisfies $\text{End}(E') \cong \mathcal{O}_H$. Hint: read the discussion surrounding [26, Proposition 3.3].

3. LENGTHS OF LOCAL RINGS

In this section we prove part (c) of Theorem 1.2.1 under the hypothesis that p is either odd or unramified in K . This formula is due to Gross [5], whose proof was based on formal group cohomology. We will give a very different proof which is based instead on Zink's theory of *displays* [33] (see also Messing's Bourbaki talk [22]).

3.1. Some notation. Fix a prime p which is nonsplit in K and let \mathfrak{p} be the prime of K above p . Let

$$W = W(\mathbb{F}_p^{\text{alg}})$$

be the ring of Witt vectors of $\mathbb{F}_p^{\text{alg}}$. For the theory of Witt vectors see Rabinoff's notes [24]. As a topological ring W is isomorphic to the integer ring of the completion of the maximal unramified extension of \mathbb{Q}_p , and W comes equipped with a canonical isomorphism $W/pW \cong \mathbb{F}_p^{\text{alg}}$. The ring W also comes equipped with two continuous functions

$$F, V : W \rightarrow W$$

denoted $x \mapsto x^F$ and $x \mapsto x^V$, respectively. The function F is the unique continuous ring automorphism which induces the absolute Frobenius $x \mapsto x^p$ on W/pW , and V is the unique additive map which satisfies $(x^V)^F = px$. The subring

$$\mathbb{Z}_{p^2} = \{x \in W \mid (x^F)^F = x\}$$

is isomorphic to the integer ring of the unramified quadratic extension of \mathbb{Q}_p .

Let \mathcal{W} be the integer ring of the completion of the maximal unramified extension of $K_{\mathfrak{p}}$ and denote by

$$(11) \quad i : \mathcal{O}_K \rightarrow \mathcal{W}.$$

the inclusion. Equivalently we could define

$$\mathcal{W} = \begin{cases} W & \text{if } p \text{ is inert in } K \\ W \otimes_{\mathbb{Z}} \mathcal{O}_K & \text{if } p \text{ is ramified in } K. \end{cases}$$

If p is unramified in K then i is the unique ring homomorphism which lifts the reduction-mod- \mathfrak{p} map $\mathcal{O}_K \rightarrow \mathbb{F}_p \rightarrow \mathbb{F}_p^{\text{alg}}$; furthermore $i(x)^F = i(\bar{x})$ and the induced map $\mathcal{O}_{K, \mathfrak{p}} \rightarrow W$ has image \mathbb{Z}_{p^2} . If p is ramified in K then $i(x) = 1 \otimes x$.

Let \mathcal{ART} be the category of Artinian local \mathcal{W} -algebras R equipped with an isomorphism $R/\mathfrak{m}_R \cong \mathbb{F}_p^{\text{alg}}$. For every object R the unique maximal ideal $\mathfrak{m}_R \subset R$ contains p and satisfies $\mathfrak{m}_R^k = 0$ for $k \gg 0$. In particular p is nilpotent in

R . A morphism in \mathcal{ART} is a ring homomorphism $f : S \rightarrow R$ which satisfies $f(\mathfrak{m}_S) \subset \mathfrak{m}_R$ and induces the identity $\mathbb{F}_p^{\text{alg}} \rightarrow \mathbb{F}_p^{\text{alg}}$ on residue fields. By virtue of the homomorphism (11) every object R of \mathcal{ART} is naturally an \mathcal{O}_K -algebra, and we denote by

$$(12) \quad i : \mathcal{O}_K \rightarrow R$$

the structure map.

3.2. Local rings and deformations.

Definition 3.2.1. Let $S \rightarrow R$ be a surjective morphism in \mathcal{ART} and suppose E is an elliptic curve over R . A *deformation* (or *lift*) of E to S is an elliptic curve \tilde{E} over S equipped with an isomorphism $\tilde{E}/_R \cong E$. Here and elsewhere, we use the notation

$$\tilde{E}/_R \stackrel{\text{def}}{=} \tilde{E} \times_{\text{Spec}(S)} \text{Spec}(R)$$

for base change.

The same notion of deformation applies to any mathematical entity for which there is a reasonable notion of base change through a surjective morphism $S \rightarrow R$. In particular we may also talk about deformations of CM elliptic curves over R , triples $(E, \kappa, j) \in \mathcal{Z}_m(R)$, and (later) about deformations of p -Barsotti-Tate groups and displays over R .

Fix $m \in \mathbb{Z}^+$ and let \mathcal{Z}_m be the restriction of the functor Z_m from \mathcal{O}_K -schemes to \mathcal{W} -schemes. Thus \mathcal{Z}_m is (coarsely) representable by the base change

$$\mathcal{Z}_m = Z_m \times_{\text{Spec}(\mathcal{O}_K)} \text{Spec}(\mathcal{W}).$$

Fix a point $z \in \mathcal{Z}_m(\mathbb{F}_p^{\text{alg}})$ corresponding to a triple (E, κ, j) in which (E, κ) is a CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$ and $j \in L(E, \kappa)$ is a special endomorphism of degree m . Let R be an object of \mathcal{ART} and suppose we are given a deformation $(\tilde{E}, \tilde{\kappa}, \tilde{j})$ of (E, κ, j) to R . The deformation $(\tilde{E}, \tilde{\kappa}, \tilde{j})$ corresponds to a point $\tilde{z} \in \mathcal{Z}_m(R)$ whose image under the reduction map

$$\mathcal{Z}_m(R) \rightarrow \mathcal{Z}_m(\mathbb{F}_p^{\text{alg}})$$

is the point z , and so we have a commutative diagram of \mathcal{W} -schemes

$$\begin{array}{ccc} \text{Spec}(\mathbb{F}_p^{\text{alg}}) & & \\ \downarrow & \searrow z & \\ \text{Spec}(R) & \xrightarrow{\tilde{z}} & \mathcal{Z}_m. \end{array}$$

As R is local the arrow \tilde{z} factors uniquely as

$$\text{Spec}(R) \rightarrow \text{Spec}(\mathcal{O}_{\mathcal{Z}_m, z}) \rightarrow \mathcal{Z}_m,$$

and so to the deformation $(\tilde{E}, \tilde{\kappa}, \tilde{j})$ we attach a homomorphism of local \mathcal{W} -algebras $\mathcal{O}_{\mathcal{Z}_m, z} \rightarrow R$. As R is Artinian this map extends uniquely to a homomorphism on the completed local ring $\hat{\mathcal{O}}_{\mathcal{Z}_m, z}$. This construction establishes a bijection

$$(13) \quad \{\text{deformations of } (E, \kappa, j) \text{ to } R\} \cong \text{Hom}_{\mathcal{W}}(\hat{\mathcal{O}}_{\mathcal{Z}_m, z}, R).$$

Remark 3.2.2. If Z_m were actually a fine moduli space then it would be obvious that (13) is a bijection, but as Z_m is only a coarse moduli space there is actually something to prove. For us it will suffice to simply say that the bijectivity of (13) is a consequence of [18, Corollary 5.2].

3.3. Barsotti-Tate groups and the Serre-Tate theorem. We recall the basic properties of p -Barsotti-Tate groups, mostly to fix notation. The main references are Shatz's survey [28] and Tate's original article [31]. Let R be an object of \mathcal{ART} .

Suppose G is a finite flat (commutative) group scheme over R . As any scheme which is finite over an affine scheme is itself affine, we have $G = \text{Spec}(A)$ for some finite flat (hence free) R -algebra A . The *order* of G is defined to be $\text{rank}_R(A)$. By [3, Corollary 7.6] the ring A decomposes as a product $A \cong A_0 \times \cdots \times A_k$ of finitely many local R -algebras. Among these local factors there is one which is distinguished: the identity element $\text{id} \in G(R)$ is a morphism $\text{id} : \text{Spec}(R) \rightarrow G$ which corresponds to an R -algebra homomorphism

$$\epsilon : A \rightarrow R.$$

There is a unique factor A_0 in the above direct product such that ϵ factors through the projection $A \rightarrow A_0$. If we set $G^0 = \text{Spec}(A_0)$ then the closed subscheme $G^0 \rightarrow G$ is in fact a closed subgroup scheme, called the *connected component of the identity*. If $G_0 = G$, i.e. if A is a local ring, then we say that G is *connected*. For each factor A_i in the above product there is an idempotent $e_i \in A$ for which $A_i = Ae_i$. For each i we obtain an injective ring homomorphism $R \rightarrow A_i$ defined by $r \mapsto re_i$. As each A_i contains a natural subring isomorphic to R , the R -algebra A contains a natural subring $A^{\text{et}} = R \times \cdots \times R$ (the maximal étale subalgebra of A). If we set $G^{\text{et}} = \text{Spec}(A^{\text{et}})$ then the inclusion $A^{\text{et}} \rightarrow A$ determines a homomorphism of finite flat group schemes $G \rightarrow G^{\text{et}}$. We say that G is *étale* if $G = G^{\text{et}}$, i.e. if $A \cong R \times \cdots \times R$. A fundamental result is that the sequence of group schemes, the *connected-étale sequence*

$$0 \rightarrow G^0 \rightarrow G \rightarrow G^{\text{et}} \rightarrow 0$$

is exact.

A p -Barsotti-Tate group (or p -divisible group) $\mathfrak{G} = \varinjlim G_k$ of *height* h over R is an inductive system

$$(14) \quad G_0 \xrightarrow{i_0} G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} \cdots$$

in which each G_k is a finite flat group scheme over R of order kh , and for every $k \geq 0$ the map i_k is a closed immersion making the sequence

$$0 \rightarrow G_k \xrightarrow{i_k} G_{k+1} \xrightarrow{p^k} G_{k+1}$$

exact. Given a p -Barsotti-Tate group $\mathfrak{G} = \varinjlim G_k$ we define two new p -Barsotti-Tate groups

$$\mathfrak{G}^0 = \varinjlim G_k^0 \quad \mathfrak{G}^{\text{et}} = \varinjlim G_k^{\text{et}}$$

by taking connected components and maximal étale quotients at each finite step G_k . We say that \mathfrak{G} is *connected* if $\mathfrak{G} = \mathfrak{G}^0$, and say that \mathfrak{G} is *étale* if $\mathfrak{G} = \mathfrak{G}^{\text{et}}$. For every k there is an R -algebra A_k such that $G_k = \text{Spec}(A_k)$, and the maps in (14) correspond to maps $A_{k+1} \rightarrow A_k$. Define the *affine coordinate ring* of \mathfrak{G} to be $\mathfrak{A} = \varprojlim A_k$. As k varies the maps $\epsilon : A_k \rightarrow R$ fit together into a single local R -algebra homomorphism $\epsilon : \mathfrak{A} \rightarrow R$.

Definition 3.3.1. Let \mathfrak{G} be p -Barsotti-Tate group over R with affine coordinate ring \mathfrak{A} . A *derivation* of \mathfrak{A} is an R -linear map $d : \mathfrak{A} \rightarrow R$ which satisfies

$$d(ab) = \epsilon(a)d(b) + \epsilon(b)d(a)$$

for all $a, b \in \mathfrak{A}$. The *Lie algebra* of \mathfrak{G} , denoted $\text{Lie}(\mathfrak{G})$ is the R -module of all derivations of \mathfrak{A} .

A fundamental result of Tate asserts that any connected p -Barsotti-Tate group over R is *formally smooth* in the following sense.

Theorem 3.3.2 (Tate). *Let \mathfrak{G} be a connected p -Barsotti-Tate group over R and let \mathfrak{A} be its affine coordinate ring. Then $\mathfrak{A} \cong R[[X_1, \dots, X_d]]$ for some $d \geq 0$.*

Exercise 3.3.3. Let \mathfrak{A} be the affine coordinate ring of a p -Barsotti-Tate group \mathfrak{G} over R and let $\mathfrak{J} = \ker(\epsilon : \mathfrak{A} \rightarrow R)$. Construct an isomorphism of R -modules

$$\text{Lie}(\mathfrak{G}) \cong \text{Hom}_R(\mathfrak{J}/\mathfrak{J}^2, R),$$

Exercise 3.3.4. Prove that for any p -Barsotti-Tate group \mathfrak{G} over R there is an isomorphism of R -modules $\text{Lie}(\mathfrak{G}) \cong \text{Lie}(\mathfrak{G}^0)$.

Exercise 3.3.5. Let \mathfrak{G} be a p -Barsotti-Tate group and let \mathfrak{A}^0 be the affine coordinate ring of \mathfrak{G}^0 . By Tate's theorem $\mathfrak{A}^0 \cong R[[X_1, \dots, X_d]]$ for some d . Prove that $\text{Lie}(\mathfrak{G})$ is a free R -module of rank d .

Definition 3.3.6. The *dimension* of a p -Barsotti-Tate group \mathfrak{G} over R is

$$\dim(\mathfrak{G}) = \text{rank}_R \text{Lie}(\mathfrak{G}).$$

To any elliptic curve E over R there is an associated p -Barsotti-Tate group

$$E_{p^\infty} = \varinjlim E[p^k]$$

of height 2 and dimension 1.

Remark 3.3.7. If the reduction of E to $\mathbb{F}_p^{\text{alg}}$ is ordinary then $E_{p^\infty}^0$ and $E_{p^\infty}^{\text{et}}$ are each of height 1. If the reduction of E to $\mathbb{F}_p^{\text{alg}}$ is supersingular then $E_{p^\infty}^0 = E_{p^\infty}$ and $E_{p^\infty}^{\text{et}} = 0$. Thus E_{p^∞} is connected if and only if the reduction of E is supersingular.

Any $f \in \text{End}(E)$ determines an $f \in \text{End}(E_{p^\infty})$.

Theorem 3.3.8 (Serre-Tate). *Suppose that E is an elliptic curve over $\mathbb{F}_p^{\text{alg}}$. The rule $\tilde{E} \mapsto \tilde{E}_{p^\infty}$ defines a bijection*

$$\{\text{deformations of } E \text{ to } R\} \rightarrow \{\text{deformations of } E_{p^\infty} \text{ to } R\}.$$

For any $f \in \text{End}(E)$ the rule $(\tilde{E}, \tilde{f}) \mapsto (\tilde{E}_{p^\infty}, \tilde{f})$ defines a bijection

$$\{\text{deformations of } (E, f) \text{ to } R\} \rightarrow \{\text{deformations of } (E_{p^\infty}, f) \text{ to } R\}.$$

Proof. See [21] or [9]. □

3.4. Dieudonné modules. We use slightly different conventions for Dieudonné modules than what is found in much of the literature. In order that our conventions agree with those of Messing and Zink [22, 33], we adopt the *covariant* conventions for Dieudonné modules rather than the *contravariant* conventions used by Demazure [2]. Nonetheless, [2] remains our main reference for this subsection.

A *Dieudonné module* over $\mathbb{F}_p^{\text{alg}}$ is a triple (D, F, V) in which D is a free W -module of finite rank, and $F, V : D \rightarrow D$ are additive homomorphisms which satisfy $FV = VF = p$ and

$$\begin{aligned} F(x \cdot m) &= x^F \cdot F(m) \\ V(x^F \cdot m) &= x \cdot V(m) \end{aligned}$$

for all $x \in W$ and $m \in D$. The *height* of D is $\text{rank}_W(D)$, the *Lie algebra* of D is the $\mathbb{F}_p^{\text{alg}}$ -vector space

$$\text{Lie}(D) = D/VD,$$

and the *dimension* of D is the $\mathbb{F}_p^{\text{alg}}$ -dimension of $\text{Lie}(D)$. We usually just say “let D be a Dieudonné module” and omit explicit reference to F and V .

One can construct Dieudonné modules as follows. Given a rational number $0 \leq \lambda \leq 1$ write $\lambda = s/t$ with $\gcd(s, t) = 1$ and define a \mathbb{Q}_p -vector space

$$\mathcal{B}_\lambda = \mathbb{Q}_p[x]/(x^t - p^s).$$

Let $F, V : \mathcal{B}_\lambda \rightarrow \mathcal{B}_\lambda$ be the \mathbb{Q}_p -linear maps determined by

$$V(m) = x \cdot m$$

and $F = pV^{-1}$. Set $\mathcal{D}_\lambda = W \otimes_{\mathbb{Z}_p} \mathcal{B}_\lambda$ and extend F and V to \mathbb{Q}_p -linear maps $\mathcal{D}_\lambda \rightarrow \mathcal{D}_\lambda$ by

$$F(x \otimes b) = x^F \otimes F(b) \quad V(x^F \otimes b) = x \otimes V(b).$$

One can construct a Dieudonné module by choosing any W -lattice in \mathcal{D}_λ which is stable under the operators F and V , as in the following exercise.

Exercise 3.4.1. Choose any $\beta_0, \dots, \beta_{t-1} \in W$ which satisfy

$$\text{ord}_p(\beta_{i+1}) \leq \text{ord}_p(\beta_i) \leq \text{ord}_p(\beta_{i+1}) + 1$$

and $\text{ord}_p(\beta_0) - \text{ord}_p(\beta_{t-1}) = s$. Show that the W -summodule

$$D = \text{Span}_W\{\beta_i \otimes x^i : 0 \leq i < t\} \subset \mathcal{D}_{s/t}$$

is stable under both F and V and so is a Dieudonné module.

Proposition 3.4.2. *Let D be a Dieudonné module over $\mathbb{F}_p^{\text{alg}}$. There is a unique sequence of rational numbers $0 \leq \lambda_1 \leq \dots \leq \lambda_k \leq 1$ for which*

$$D \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{1 \leq i \leq k} \mathcal{D}_{\lambda_i}$$

in a way respecting the actions of W , F , and V on both sides. If $\lambda_i = s_i/t_i$ then D has dimension $\sum s_i$ and height $\sum t_i$.

Proof. See [2, Chapter IV]. □

Definition 3.4.3. The rational numbers (counted with multiplicity) $\{\lambda_1, \dots, \lambda_k\}$ are the *slopes* of D .

Theorem 3.4.4. *There is a covariant equivalence $\mathfrak{G} \mapsto D(\mathfrak{G})$ from the category of p -Barsotti-Tate groups over $\mathbb{F}_p^{\text{alg}}$ to the category of Dieudonné modules over $\mathbb{F}_p^{\text{alg}}$. This equivalence satisfies*

$$\begin{aligned} \dim(\mathfrak{G}) &= \dim(D(\mathfrak{G})) \\ \text{height}(\mathfrak{G}) &= \text{height}(D(\mathfrak{G})) \\ \text{Lie}(\mathfrak{G}) &\cong \text{Lie}(D(\mathfrak{G})). \end{aligned}$$

Furthermore \mathfrak{G} is étale if and only if all slopes of $D(\mathfrak{G})$ are equal to 0, and \mathfrak{G} is connected if and only if all slopes of $D(\mathfrak{G})$ are nonzero.

Proof. See [2, Chapter IV]. \square

Remark 3.4.5. One may restate the final claim of Theorem 3.4.4 as follows: a p -Barsotti-Tate group \mathfrak{G} over $\mathbb{F}_p^{\text{alg}}$ is connected if and only if V is topologically nilpotent on $D(\mathfrak{G})$.

Exercise 3.4.6. Let $\pi \in \mathbb{Z}_p$ be a uniformizing parameter and consider the Dieudonné module $D = W$ with operators

$$F(x) = \pi x^F \quad V(x^F) = \frac{p}{\pi} x.$$

Show that D has dimension 0 and height 1, and that D does not depend on the choice of π . By classifying all F and V stable W -lattices in \mathcal{D}_0 , show that D is the unique Dieudonné module of dimension 0 and height 1. Deduce that $D \cong D(\mathbb{Q}_p/\mathbb{Z}_p)$.

Exercise 3.4.7. Let $\pi \in \mathbb{Z}_p$ be a uniformizing parameter and consider the Dieudonné module $D = W$ with operators

$$F(x) = \frac{p}{\pi} x^F \quad V(x^F) = \pi x.$$

Show that D has dimension 1 and height 1, and that D does not depend on the choice of π . By classifying all F and V stable W -lattices in \mathcal{D}_1 , show that D is the unique Dieudonné module of dimension 1 and height 1. Deduce that $D \cong D(\mu_{p^\infty})$.

Remark 3.4.8. If E is an elliptic curve over $\mathbb{F}_p^{\text{alg}}$ then $D(E_{p^\infty})$ has dimension one and height two. The only possible slopes are $\{0, 1\}$ and $\{1/2\}$. The first occurs when E is ordinary, the second occurs when E is supersingular.

Definition 3.4.9. Define the *supersingular Dieudonné module* D_{ss} as follows. Fix a uniformizing parameter $\pi \in \mathbb{Z}_p$. As a W -module D_{ss} is free on two generators $\{e_1, e_2\}$. The operators F and V on $\{e_1, e_2\}$ are determined by

$$F(e_1) = e_2 \quad F(e_2) = \pi e_1$$

and

$$V(e_1) = \frac{p}{\pi} e_2 \quad V(e_2) = p e_1.$$

Exercise 3.4.10. Prove that D_{ss} does not depend on the choice of π , and that D_{ss} is the unique Dieudonné module of slopes $\{1/2\}$.

Exercise 3.4.11. Prove that the endomorphism ring of D_{ss} is

$$\text{End}(D_{\text{ss}}) \cong \left\{ \begin{pmatrix} a & \pi b \\ b^F & a^F \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\}.$$

3.5. Displays. In order to study the deformation theory of p -Barsotti-Tate groups we need an equivalence of categories, in the spirit of Theorem 3.4.4, which holds over more general rings than $\mathbb{F}_p^{\text{alg}}$. The correct category is provided by Zink's theory of *displays* [22, 33].

Fix an object R of \mathcal{ART} and let $W(R)$ be the ring of Witt vectors of R (for Witt vectors see Rabinoff's notes [24]). There is a canonical surjection $W(R) \rightarrow R$ whose kernel we denote by

$$I_R = \ker(W(R) \rightarrow R).$$

The ring $W(R)$ is equipped with a ring endomorphism

$$F : W(R) \rightarrow W(R)$$

and an isomorphism of additive groups

$$V : W(R) \rightarrow I_R$$

(denoted $x \mapsto x^F$ and $x \mapsto x^V$, respectively) which are related by $(x^V)^F = px$. Note that in general the operators F and V do not commute.

Definition 3.5.1. A *display* over R is a quadruple (P, Q, F, F_1) in which P is a free $W(R)$ -module of finite rank, $Q \subset P$ is a $W(R)$ -submodule, and $F : P \rightarrow P$ and $F_1 : Q \rightarrow P$ are additive maps which satisfy

$$F(x \cdot a) = x^F \cdot F(a) \quad F_1(x \cdot b) = x^F \cdot F_1(b)$$

for all $x \in W(R)$, $a \in P$, and $b \in Q$. The quadruple (P, Q, F, F_1) is required to satisfy the following addition properties:

- (a) $I_R P \subset Q$,
- (b) P/Q is a free R -module,
- (c) P is generated as a $W(R)$ -module by $F_1(Q)$,
- (d) $F_1(x^V \cdot a) = x \cdot F(a)$ for all $x \in W(R)$ and all $a \in P$.

By abuse of notation we will sometimes say “let P be a display” and suppress the data Q , F , and F_1 from the notation. The *Lie algebra* of P is the free R -module

$$\text{Lie}(P) = P/Q,$$

the *dimension* of P is $\text{rank}_R(\text{Lie}(P))$, and the *height* of P is $\text{rank}_{W(R)}(P)$.

Remark 3.5.2. Zink writes V^{-1} instead of F_1 . To see why, look at Exercise 3.5.4. Also, what we call a display is called a 3n-display in [33]. The “3n” stands for not-necessarily-nilpotent. Our notation and definition agree with Messing's article [22].

Definition 3.5.3. A *CM display* over an object R of \mathcal{ART} is a pair (P, κ) in which P is a display over R of height two and dimension one, and $\kappa : \mathcal{O}_K \rightarrow \text{End}(P)$ is an action such that the induced action of \mathcal{O}_K on $\text{Lie}(P)$ is through (12).

Exercise 3.5.4. Given a Dieudonné module D over $\mathbb{F}_p^{\text{alg}}$ the operator V defines a bijection $D \rightarrow VD$, and we may attach to D the display (D, VD, F, V^{-1}) . Show that the construction

$$(D, F, V) \mapsto (D, VD, F, V^{-1})$$

defines an equivalence between the category of Dieudonné modules over $\mathbb{F}_p^{\text{alg}}$ and the category of displays over $\mathbb{F}_p^{\text{alg}}$.

Example 3.5.5. We may apply the construction of Exercise 3.5.4 to the supersingular Dieudonné module D_{ss} of Definition 3.4.9. The associated display over $\mathbb{F}_p^{\text{alg}}$ is $(P_{\text{ss}}, Q, F, F_1)$ in which P_{ss} is the free W -module on two generators $\{e_1, e_2\}$, Q is the submodule spanned by $\{\pi e_1, e_2\}$, $F : P_{\text{ss}} \rightarrow P_{\text{ss}}$ satisfies

$$F(e_1) = e_2 \quad F(e_2) = \pi e_1$$

and $F_1 : Q \rightarrow P_{\text{ss}}$ satisfies

$$F_1(\pi e_1) = e_2 \quad F_1(e_2) = \frac{\pi}{p} e_1.$$

By Exercise 3.4.11 the endomorphism ring of P_{ss} is

$$\text{End}(P_{\text{ss}}) \cong \left\{ \begin{pmatrix} a & \pi b \\ b^F & a^F \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\}.$$

Given a morphism $S \rightarrow R$ in \mathcal{ART} and a display P over S one can define the *base change* P/R as in [33, Definition 20]. In particular if $S \rightarrow R$ is a surjection and we start with a display P over R , then it makes sense to talk about deformations of P to S , as in Definition 3.2.1.

Definition 3.5.6. Let R be an object of \mathcal{ART} and let P be a display over R . By Exercise 3.5.4 the base change $P/\mathbb{F}_p^{\text{alg}}$ corresponds to a Dieudonné module D over $\mathbb{F}_p^{\text{alg}}$. We say that the display P is *nilpotent* if the operator V on D is topologically nilpotent.

Theorem 3.5.7 (Zink). *Let R be an object of \mathcal{ART} . There is an equivalence $\mathfrak{G} \mapsto P(\mathfrak{G})$ between the category of connected p -Barsotti-Tate groups over R and the category of nilpotent displays over R .*

Proof. This is [33, Theorem 9]. □

If $S \rightarrow R$ is a morphism in \mathcal{ART} and \mathfrak{G} is a connected p -Barsotti-Tate group over R then Zink's equivalence of categories induces a bijection

$$\{\text{deformations of } \mathfrak{G} \text{ to } S\} \cong \{\text{deformations of } P(\mathfrak{G}) \text{ to } S\}.$$

When combined with the Serre-Tate theorem we obtain the following result. Let (E, κ) be a CM elliptic curve over R whose reduction to $\mathbb{F}_p^{\text{alg}}$ is supersingular, and let $P = P(E_{p^\infty})$ be the associated display over R . There is canonical bijection

$$(15) \quad \{\text{deformations of } (E, \kappa) \text{ to } S\} \cong \{\text{deformations of } (P, \kappa) \text{ to } S\}.$$

Furthermore if $j \in \text{End}(E)$ and endomorphism then there is a corresponding endomorphism $j \in \text{End}(P)$ and a canonical bijection

$$(16) \quad \{\text{deformations of } (E, \kappa, j) \text{ to } S\} \cong \{\text{deformations of } (P, \kappa, j) \text{ to } S\}.$$

3.6. Crystalline deformation theory. Given a surjective morphism $S \rightarrow R$ in \mathcal{ART} and a nilpotent display P over R it is typically difficult to determine all deformations of P to S . However for certain special surjections $S \rightarrow R$ Zink has an elegant theory which describes such deformations in a very concrete way.

Definition 3.6.1. Suppose S is a ring and $\mathfrak{a} \subset S$ is an ideal. A *divided power structure* on \mathfrak{a} is a collection of functions

$$\gamma_\bullet = \{\gamma_n : \mathfrak{a} \rightarrow \mathfrak{a}\}_{n \in \mathbb{Z}^+}$$

satisfying the following properties for all $m, n \in \mathbb{Z}^+$, $s, t \in S$, and $x, y \in \mathfrak{a}$:

$$(17) \quad \gamma_n(sx) = s^n \gamma(x)$$

$$(18) \quad \gamma_m(x) \cdot \gamma_n(x) = \frac{(m+n)!}{m!n!} \cdot \gamma_{m+n}(x)$$

$$(19) \quad \gamma_n(x+y) = \gamma_n(x) + \left(\sum_{i=1}^{n-1} \gamma_{n-i}(x) \gamma_i(y) \right) + \gamma_n(y)$$

$$(20) \quad \gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!} \cdot \gamma_{mn}(x).$$

Remark 3.6.2. The axioms for a divided power structure are intended to encode the idea that $\gamma_n(x)$ behaves like $x^n/n!$, and the motivation for defining a divided power structure in the first place is so that one can imitate the construction of the exponential function in situations where the expression $x^n/n!$ doesn't make sense. For example if one has the additional property that $\gamma_n = 0$ for $n \gg 0$ then the function

$$\exp(x) = 1 + \sum_{i=1}^{\infty} \gamma_i(x)$$

defines an isomorphism of groups $\mathfrak{a} \rightarrow 1 + \mathfrak{a}$ (see [21, p.79]).

Example 3.6.3. For any $n \in \mathbb{Z}^+$ we have $p^n/n! \in p\mathbb{Z}$. Thus if S is any ring there is a canonical divided power structure on the ideal pS defined by

$$\gamma_n(px) = \frac{p^n}{n!} \cdot x^n.$$

Definition 3.6.4. A *PD-thickening* is a surjective morphism $S \rightarrow R$ in \mathcal{ART} together with a divided power structure γ_\bullet on the ideal $\mathfrak{a} = \ker(S \rightarrow R)$. We further require that the restriction of γ_\bullet to $\mathfrak{a} \cap pS$ agree with the canonical divided power structure of Example 3.6.3.

The following three examples are the only examples of PD-thickenings we will ever need.

Example 3.6.5. Suppose $S \rightarrow R$ is a surjective morphism in \mathcal{ART} whose kernel $\mathfrak{a} = \ker(S \rightarrow R)$ satisfies $\mathfrak{a}^2 = \mathfrak{a}$. Then we may equip \mathfrak{a} with the *trivial divided powers* defined by

$$\gamma_1(x) = x$$

and $\gamma_n(x) = 0$ for $n > 1$. This makes $S \rightarrow R$ into a PD-thickening.

Example 3.6.6. Suppose p is unramified in K and let $\mathfrak{m} = p\mathcal{W}$ be the maximal ideal of \mathcal{W} . For any $k \in \mathbb{Z}^+$ the surjection

$$\mathcal{W}/\mathfrak{m}^k \rightarrow \mathbb{F}_p^{\text{alg}}$$

has kernel $\mathfrak{a} = \mathfrak{m}/\mathfrak{m}^k$ generated by p , and so the canonical divided power structure on \mathfrak{a} is the unique divided power structure making $\mathcal{W}/\mathfrak{m}^k \rightarrow \mathbb{F}_p^{\text{alg}}$ into a PD-thickening.

Example 3.6.7. Suppose $p \neq 2$ is ramified in K and let $\varpi \in \mathcal{O}_{K,p}$ be a uniformizer. Then $\mathfrak{m} = i(\varpi)$ is the maximal ideal of \mathcal{W} . For any $k \in \mathbb{Z}^+$ the surjection $\mathcal{W}/\mathfrak{m}^k \rightarrow \mathbb{F}_p^{\text{alg}}$ has kernel $\mathfrak{a} = \mathfrak{m}/\mathfrak{m}^k$ generated by $i(\varpi)$. By the following exercise the ideal \mathfrak{a} is equipped with the divided power structure

$$\gamma_n(i(\varpi)x) = \frac{i(\varpi^n)}{n!} \cdot x^n,$$

and this divided power structure makes $\mathcal{W}/\mathfrak{m}^k \rightarrow \mathbb{F}_p^{\text{alg}}$ into a PD-thickening.

Exercise 3.6.8. Prove that for any $n \in \mathbb{Z}^+$ we have.

$$\text{ord}_p(n!) \leq \frac{n-1}{p-1}$$

(hint: see [7, IV.1.3]). Deduce that if p is odd and ramified in K then for any uniformizer $\varpi \in \mathcal{O}_{K,p}$

$$\varpi^n/n! \in \varpi\mathcal{O}_{K,p}.$$

Remark 3.6.9. As has already been noted, we will only prove part (c) of Theorem 1.2.1 under the hypothesis that either p is unramified in K or $p \neq 2$. Our methods break down when $p = 2$ is ramified in K precisely because of the necessity of $p \neq 2$ in the preceding exercise.

Suppose R is an object of \mathcal{ART} and (P, Q, F, F_1) is a display over R . The *Hodge sequence* of (P, Q, F, F_1) is the short exact sequence of R -modules

$$0 \rightarrow Q/I_R P \rightarrow P/I_R P \rightarrow P/Q \rightarrow 0.$$

Note that $P/I_R P$ and P/Q are free R -modules by hypothesis, and in particular the Hodge sequence splits (noncanonically). From this it follows that $Q/I_R P$ is a projective R -module, and hence also free (as R is local). The submodule

$$Q/I_R P \subset P/I_R P$$

is the *Hodge filtration* of $P/I_R P$. In anticipation of coming events we abbreviate

$$\mathbf{P}(R) = P/I_R P$$

so that the Hodge sequence takes the form

$$0 \rightarrow Q/I_R P \rightarrow \mathbf{P}(R) \rightarrow \text{Lie}(P) \rightarrow 0.$$

Suppose $S \rightarrow R$ is a PD-thickening and P is a nilpotent display over R . Central to Zink's deformation theory is the following fact [33, Theorem 44]: given any two deformations \tilde{P}_1, \tilde{P}_2 of P to S there is a canonical isomorphism of S -modules (which depends on the divided power structure on $\ker(S \rightarrow R)$)

$$(21) \quad \tilde{P}_1/I_S \tilde{P}_1 \cong \tilde{P}_2/I_S \tilde{P}_2.$$

Thus if we define a free S -module of rank height(P)

$$\mathbf{P}(S) \stackrel{\text{def}}{=} \tilde{P}/I_S \tilde{P}$$

for *any* deformation \tilde{P} of P to S , the result does not depend on which deformation we choose, and furthermore satisfies

$$(22) \quad \mathbf{P}(S) \otimes_S R \cong \mathbf{P}(R).$$

The rule $S \mapsto \mathbf{P}(S)$ is the *crystal* of the display P (more precisely, it is the *covariant Dieudonné crystal* of [33, Definition 47]). This rule assigns to every PD-thickening

$S \rightarrow R$ a lifting of the R -module $\mathbf{P}(R)$ to an S -module $\mathbf{P}(S)$ (*lifting* just means that the relation (22) holds). The isomorphism (21) need not preserve the Hodge filtration, and so the submodule

$$\tilde{Q}/I_S\tilde{P} \subset \mathbf{P}(S)$$

does depend on the choice of deformation \tilde{P} . The rule

$$\tilde{P} \mapsto \tilde{Q}/I_S\tilde{P}$$

therefore defines an interesting function from the set of all deformations of P to the set of all direct summands $\mathcal{L} \subset \mathbf{P}(S)$ which lift the Hodge filtration of $\mathbf{P}(R)$:

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & \mathbf{P}(S) \\ \downarrow & & \downarrow \\ Q/I_R P & \longrightarrow & \mathbf{P}(R). \end{array}$$

To be precise, by a lifting the Hodge filtration of $\mathbf{P}(R)$ we mean a direct summand $\mathcal{L} \subset \mathbf{P}(S)$ such that the isomorphism (21) identifies $\mathcal{L} \otimes_S R \cong Q/I_R P$.

The following result is Zink's version of the Grothendieck-Messing deformation theory [7, 21].

Theorem 3.6.10 (Zink). *As above, let $S \rightarrow R$ be a PD-thickening and let P be a nilpotent display over R . The function $\tilde{P} \mapsto \tilde{Q}/I_S\tilde{P}$ defines a bijection between deformations of P to S and liftings of the Hodge filtration:*

$$\begin{array}{ccc} \tilde{Q}/I_S\tilde{P} & \longrightarrow & \mathbf{P}(S) \\ \downarrow & & \downarrow \\ Q/I_R P & \longrightarrow & \mathbf{P}(R). \end{array}$$

Moreover, any endomorphism $f \in \text{End}(P)$ induces a canonical S -linear map

$$\mathbf{f}_S : \mathbf{P}(S) \rightarrow \mathbf{P}(S)$$

such that:

- (a) \mathbf{f}_S lifts the map $\mathbf{f}_R : \mathbf{P}(R) \rightarrow \mathbf{P}(R)$ induced by f ,
- (b) $f \in \text{End}(P)$ lifts to an endomorphism $\tilde{f} \in \text{End}(\tilde{P})$ if and only if

$$\mathbf{f}_S(\tilde{Q}/I_S\tilde{P}) \subset \tilde{Q}/I_S\tilde{P}.$$

In other words if \tilde{P} is the deformation corresponding to the lift of the Hodge filtration $\mathcal{L} \subset \mathbf{P}(S)$ then the endomorphism f lifts to an endomorphism of \tilde{P} if and only if $\mathbf{f}_S(\mathcal{L}) \subset \mathcal{L}$.

Proof. This is [33, Proposition 45]. □

3.7. Deforming CM elliptic curves. If R is any object of \mathcal{ART} then let J_R be the kernel of the ring homomorphism

$$\tau_R : \mathcal{O}_K \otimes_{\mathbb{Z}} R \rightarrow R$$

defined by $\tau_R(x \otimes r) = i(x) \cdot r$. Thus there is a short exact sequence of R -modules

$$0 \rightarrow J_R \rightarrow \mathcal{O}_K \otimes_{\mathbb{Z}} R \xrightarrow{\tau_R} R \rightarrow 0.$$

This sequence is obviously split (R is projective as a module over itself), and so the R -module J_R is a direct summand of a free module. Therefore J_R is projective, and as R is local J_R is itself free of rank one. If M is a free R -module of finite type equipped with an action $\kappa : \mathcal{O}_K \rightarrow \text{End}_R(M)$ then $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ acts on M in an obvious way, and so there is a natural \mathcal{O}_K -stable R -submodule

$$J_R M \subset M.$$

Lemma 3.7.1. *Suppose M is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -module of rank one and that \mathcal{L} is an $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -submodule such that \mathcal{L} and M/\mathcal{L} are both free R -modules of rank one. Assume further that the action of \mathcal{O}_K on the quotient M/\mathcal{L} is through the map (12). Then*

$$\mathcal{L} = J_R M.$$

Proof. Let $q : M \rightarrow M/\mathcal{L}$ be the quotient map. To say that the action of \mathcal{O}_K on the quotient M/\mathcal{L} is through the map (12) means that

$$q((x \otimes r) \cdot m) = i(x) \cdot r \cdot q(m) = \tau(x \otimes r) \cdot q(m).$$

In particular if $j \in J_R$ then for any $m \in M$ we have

$$q(j \cdot m) = \tau_R(j) \cdot m = 0.$$

Therefore $J_R M \subset \mathcal{L}$. As $M \cong \mathcal{O}_K \otimes_{\mathbb{Z}} R$ as $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -modules, the comments preceding the lemma show that $J_R M$ and $M/J_R M$ are each free R -modules of rank one. Now consider the exact sequence

$$0 \rightarrow \mathcal{L}/J_R M \rightarrow M/J_R M \rightarrow M/\mathcal{L} \rightarrow 0.$$

If we fix isomorphisms of R -modules $M/J_R M \cong R$ and $M/\mathcal{L} \cong R$ then the map $M/J_R M \rightarrow M/\mathcal{L}$ is multiplication by some $r \in R$. The surjectivity of this map implies that $r \in R^\times$, and so the map is also injective. Therefore $\mathcal{L}/J_R M = 0$. \square

Exercise 3.7.2. Suppose that $S \rightarrow R$ is a surjection in \mathcal{ART} . Suppose that M is a free $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -module of rank one and \tilde{M} is an $\mathcal{O}_K \otimes_{\mathbb{Z}} S$ -module which is free over S and satisfies

$$\tilde{M} \otimes_S R \cong M$$

as $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -modules. Then \tilde{M} is free of rank one over $\mathcal{O}_K \otimes_{\mathbb{Z}} S$.

Let P_{ss} be the supersingular display over $\mathbb{F}_p^{\text{alg}}$ of Example 3.5.5. In all that follows $\kappa_{\text{ss}} : \mathcal{O}_K \rightarrow \text{End}(P_{\text{ss}})$ will denote an action such that the induced action of \mathcal{O}_K on $\text{Lie}(P_{\text{ss}})$ is through $i : \mathcal{O}_K \rightarrow \mathbb{F}_p^{\text{alg}}$. The action κ_{ss} makes the crystal $\mathbf{P}_{\text{ss}}(\mathbb{F}_p^{\text{alg}})$ into an \mathcal{O}_K -module.

Exercise 3.7.3. With $(P_{\text{ss}}, \kappa_{\text{ss}})$ as above, show that the crystal $\mathbf{P}_{\text{ss}}(\mathbb{F}_p^{\text{alg}})$ is free of rank one over $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{F}_p^{\text{alg}}$.

Proposition 3.7.4. *For any object R of \mathcal{ART} there is a unique deformation of $(P_{\text{ss}}, \kappa_{\text{ss}})$ to R .*

Proof. Set $R_k = R/\mathfrak{m}_R^k$. The natural surjection $R_{k+1} \rightarrow R_k$ has kernel

$$\mathfrak{a} = \mathfrak{m}_R^k / \mathfrak{m}_R^{k+1}.$$

As $\mathfrak{a}^2 = 0$, Example 3.6.5 shows that $R_{k+1} \rightarrow R_k$ is a PD-thickening. Set

$$(P_0, \kappa_0) = (P_{\text{ss}}, \kappa_{\text{ss}}).$$

Let us first try to lift the CM display (P_0, κ_0) over R_0 to a CM display (P_1, κ_1) over R_1 . By Exercise 3.7.3 the crystal $\mathbf{P}_0(R_0)$ is free of rank one over $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{F}_{\mathfrak{p}}^{\text{alg}}$, and by Lemma 3.7.1 the Hodge filtration of $\mathbf{P}_0(R_0)$ is

$$J_{R_0} \mathbf{P}_0(R_0) \subset \mathbf{P}_0(R_0).$$

The action κ_0 of \mathcal{O}_K on P_0 induces an action on the crystal $\mathbf{P}_0(R_1)$ (this is part of Theorem 3.6.10), and we must find all \mathcal{O}_K -stable lifts of the Hodge filtration

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & \mathbf{P}_0(R_1) \\ \downarrow & & \downarrow \\ J_{R_0} \mathbf{P}_0(R_0) & \longrightarrow & \mathbf{P}_0(R_0). \end{array}$$

By Exercise 3.7.2 the crystal $\mathbf{P}_0(R_1)$ is free of rank one over $\mathcal{O}_K \otimes_{\mathbb{Z}} R_1$, and again applying Lemma 3.7.1 shows that the only choice for \mathcal{L} is

$$\mathcal{L} = J_{R_1} \mathbf{P}_0(R_1).$$

We have now shown that (P_0, κ_0) admits a unique deformation (P_1, κ_1) to R_1 , and furthermore

$$\mathbf{P}_1(R_1) \cong P_1/I_{R_1}P_1 \cong \mathbf{P}_0(R_1)$$

is free of rank one over $\mathcal{O}_K \otimes_{\mathbb{Z}} R_1$. Now repeat the argument to show that (P_1, κ_1) admits a unique deformation to R_2 , and so on. As $\mathfrak{m}_R^k = 0$ for $k \gg 0$, we eventually find that (P_0, κ_0) admits a unique deformation to $R_k = R$. \square

Corollary 3.7.5. *Let R be an object of \mathcal{ART} . If (E, κ) is a supersingular CM elliptic curve over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$ then there is a unique deformation of (E, κ) to R .*

Proof. Let $P = P(E_{p^\infty})$ be the display associated to E_{p^∞} and let κ be the action of \mathcal{O}_K on P induced by the action of \mathcal{O}_K on E . After fixing an isomorphism $P \cong P_{\text{ss}}$ (which is possible by Exercise 3.4.10) the action $\kappa : \mathcal{O}_K \rightarrow \text{End}(P)$ corresponds to an action $\kappa_{\text{ss}} : \mathcal{O}_K \rightarrow \text{End}(P_{\text{ss}})$. By (15) there is a bijection between deformations of (E, κ) and deformations of $(P_{\text{ss}}, \kappa_{\text{ss}})$, and so the preceding proposition shows that (E, κ) admits a unique deformation to R . \square

Corollary 3.7.6. *Fix a place v of K^{alg} above \mathfrak{p} . Reduction modulo v defines a bijection between the set of all CM elliptic curves over K^{alg} and the set of all CM elliptic curves over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$.*

Proof. Let \mathbb{C}_p be the metric completion of an algebraic closure of \mathbb{Q}_p and fix a continuous ring embedding $\mathcal{W} \rightarrow \mathbb{C}_p$. Given a CM elliptic curve (E, κ) over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$, for every quotient $\mathcal{W}/\mathfrak{m}^k$ of \mathcal{W} we have proved that there is a unique deformation of (E, κ) to $\mathcal{W}/\mathfrak{m}^k$. We deduce from the discussion following [1, Theorem 3.4] that there is a unique deformation $(\tilde{E}, \tilde{\kappa})$ of (E, κ) to \mathcal{W} . From this it follows easily that (E, κ) has a unique deformation to \mathbb{C}_p . By the theory of complex multiplication (as in [30]) a CM elliptic curve over a field of characteristic zero has a model over an algebraic extension of \mathbb{Q} , and so once we fix an embedding $K^{\text{alg}} \rightarrow \mathbb{C}_p$ we find that this unique deformation is defined over K^{alg} . \square

Corollary 3.7.7. *The action of $\text{Pic}(\mathcal{O}_K)$ on the set of all CM elliptic curves over $\mathbb{F}_{\mathfrak{p}}^{\text{alg}}$ is simply transitive.*

Proof. Combine Corollary 3.7.6 with Exercise 2.1.1. \square

3.8. The unramified calculation. Assume that p is inert in K and fix a uniformizer $\pi \in \mathbb{Z}_p$. Recall that the supersingular display P_{ss} over $\mathbb{F}_p^{\text{alg}}$ has endomorphism ring

$$\text{End}(P_{\text{ss}}) \cong \left\{ \begin{pmatrix} a & \pi b \\ b^F & a^F \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\}.$$

Define an action $\kappa_{\text{ss}} : \mathcal{O}_{K,p} \rightarrow \text{End}(P_{\text{ss}})$ by

$$\kappa_{\text{ss}}(x) = \begin{pmatrix} i(x) & \\ & i(\bar{x}) \end{pmatrix}.$$

Exercise 3.8.1. Suppose that (E, κ) is a supersingular CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$ and abbreviate P for the display $P(E_{p^\infty})$. There is an isomorphism of CM displays

$$(P, \kappa) \cong (P_{\text{ss}}, \kappa_{\text{ss}}).$$

Hint: by the Noether-Skolem theorem any two embeddings $K_p \rightarrow \text{End}(P_{\text{ss}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ are conjugate.

Let $\mathfrak{m} = p\mathcal{W}$ be the maximal ideal of \mathcal{W} .

Proposition 3.8.2. *Let $(\tilde{P}_{\text{ss}}, \tilde{\kappa}_{\text{ss}})$ be the unique deformation of $(P_{\text{ss}}, \kappa_{\text{ss}})$ to $R = \mathcal{W}/\mathfrak{m}^k$. A nonzero endomorphism*

$$j = \begin{pmatrix} & \pi b \\ b^F & \end{pmatrix}$$

of P_{ss} lifts to an endomorphism of \tilde{P}_{ss} if and only if

$$k \leq \frac{\text{ord}_p(bb^F) + 2}{2}.$$

Proof. Recall that $W = \mathcal{W}$, as we assume that p is inert in K . By Example 3.6.6 the map $R \rightarrow \mathbb{F}_p^{\text{alg}}$ is a PD-thickening. Applying [33, Proposition 51] to the trivial PD-thickening $\mathbb{F}_p^{\text{alg}} \rightarrow \mathbb{F}_p^{\text{alg}}$ gives a canonical isomorphism

$$\varinjlim \mathbf{P}_{\text{ss}}(W/p^i W) \cong P_{\text{ss}}.$$

Applying $\otimes_W R$ to both sides provides a canonical isomorphism of W -modules

$$\mathbf{P}_{\text{ss}}(R) \cong P_{\text{ss}} \otimes_W R.$$

In particular

$$(23) \quad \mathbf{P}_{\text{ss}}(R) \cong P_{\text{ss}}/p^k P_{\text{ss}}.$$

Under this isomorphism the R -module endomorphism

$$\mathbf{j}_R : \mathbf{P}_{\text{ss}}(R) \rightarrow \mathbf{P}_{\text{ss}}(R)$$

corresponds to the reduction modulo p^k of j

$$j : P_{\text{ss}}/p^k P_{\text{ss}} \rightarrow P_{\text{ss}}/p^k P_{\text{ss}}.$$

Recalling that $Q = \langle pe_1, e_2 \rangle \subset P$, it is clear that the Hodge filtration $Q/pP_{\text{ss}} \subset P_{\text{ss}}/pP_{\text{ss}}$ is generated by e_2 . Thus there is an obvious lift of the Hodge filtration

$$\begin{array}{ccc} \langle e_2 \rangle & \longrightarrow & \mathbf{P}_{\text{ss}}(R) \\ \downarrow & & \downarrow \\ \langle e_2 \rangle & \longrightarrow & \mathbf{P}_{\text{ss}}(\mathbb{F}_p^{\text{alg}}). \end{array}$$

From our explicit choice of κ_{ss} it is clear that the action of \mathcal{O}_K on P_{ss} stabilizes the line We_2 , and so the isomorphism (23) shows that the action of \mathcal{O}_K on $\mathbf{P}_{\text{ss}}(W/p^k W)$ stabilizes the submodule $\langle e_2 \rangle \subset \mathbf{P}_{\text{ss}}(W/p^k W)$. In other words we have identified the (unique) \mathcal{O}_K -stable lift of the Hodge filtration which corresponds to the deformation $(\tilde{P}_{\text{ss}}, \tilde{\kappa}_{\text{ss}})$: it is simply the submodule $\langle e_2 \rangle \subset \mathbf{P}_{\text{ss}}(W/p^k W)$. Thus the following are equivalent:

- (a) j lifts to an endomorphism of $(\tilde{P}_{\text{ss}}, \tilde{\kappa}_{\text{ss}})$
- (b) \mathbf{j} preserves the Hodge filtration of $\mathbf{P}_{\text{ss}}(\mathcal{W}/p^k \mathcal{W})$
- (c) the action of j on $P_{\text{ss}}/p^k P_{\text{ss}}$ preserves the W -span of e_2 .

This last condition is equivalent to the conditions

$$\begin{aligned} j(e_2) \in We_2 + p^k P_{\text{ss}} &\iff pbe_1 \in We_2 + p^k P_{\text{ss}} \\ &\iff pbe_1 \in p^k P_{\text{ss}} \\ &\iff \text{ord}_p(bb^F) \geq 2k - 2. \end{aligned}$$

□

Proposition 3.8.3. *Suppose we have a triple $(E, \kappa, j) \in \mathcal{Z}_m(\mathbb{F}_p^{\text{alg}})$ and set*

$$k = \frac{\text{ord}_p(m) + 1}{2}.$$

The triple (E, κ, j) deforms to $\mathcal{W}/\mathfrak{m}^k$ but not to $\mathcal{W}/\mathfrak{m}^{k+1}$.

Proof. Let (P, κ) be the CM display over $\mathbb{F}_p^{\text{alg}}$ corresponding to (E_{p^∞}, κ) , and fix an isomorphism $(P, \kappa) \cong (P_{\text{ss}}, \kappa_{\text{ss}})$. The endomorphism j corresponds to an endomorphism

$$j = \begin{pmatrix} a & pb \\ b^F & a^F \end{pmatrix}$$

of P_{ss} , and the condition that j be a special endomorphism of (E, κ) is equivalent to the condition $a = 0$. In particular

$$m = j \circ j = pbb^F.$$

Thus

$$k = \frac{\text{ord}_p(m) + 1}{2} = \frac{\text{ord}_p(bb^F) + 2}{2}$$

and by Proposition 3.8.2 the triple $(P_{\text{ss}}, \kappa_{\text{ss}}, j)$ deforms to $\mathcal{W}/\mathfrak{m}^k$ but not to $\mathcal{W}/\mathfrak{m}^{k+1}$. By (16) the same is true of (E, κ, j) . □

3.9. The ramified calculation. Assume that p is ramified in K and that $p \neq 2$. In this case we may choose a uniformizer $\varpi \in \mathcal{O}_{K,p}$ satisfying $\overline{\varpi} = -\varpi$. Set $\pi = \varpi^2$ so that π is a uniformizer of \mathbb{Z}_p . As the norm map $\mathbb{Z}_{p^2}^\times \rightarrow \mathbb{Z}_p^\times$ is surjective there is a $u \in \mathbb{Z}_{p^2}^\times$ such that

$$\varpi^2 = \pi = p \cdot uu^F.$$

Recall that the supersingular display P_{ss} over $\mathbb{F}_p^{\text{alg}}$ has endomorphism ring

$$\text{End}(P_{\text{ss}}) \cong \left\{ \begin{pmatrix} a & \pi b \\ b^F & a^F \end{pmatrix} : a, b \in \mathbb{Z}_{p^2} \right\}.$$

There is a unique action $\kappa_{\text{ss}} : \mathcal{O}_K \rightarrow \text{End}(P_{\text{ss}})$ with the property

$$\kappa_{\text{ss}}(\varpi) = \begin{pmatrix} & \pi \\ 1 & \end{pmatrix}.$$

Exercise 3.9.1. Suppose that (E, κ) is a supersingular CM elliptic curve over $\mathbb{F}_p^{\text{alg}}$ and abbreviate P for the display $P(E_{p^\infty})$. There is an isomorphism of CM displays

$$(P, \kappa) \cong (P_{\text{ss}}, \kappa_{\text{ss}}).$$

Let $\mathfrak{m} = i(\varpi)\mathcal{W}$ be the maximal ideal of \mathcal{W} .

Exercise 3.9.2. Show that for any object R of \mathcal{ART} the ideal $J_R \subset \mathcal{O}_K \otimes_{\mathbb{Z}} R$ is generated as an R -module by $\varpi \otimes 1 - 1 \otimes i(\varpi)$.

Proposition 3.9.3. *Let $(\tilde{P}_{\text{ss}}, \tilde{\kappa}_{\text{ss}})$ be the unique deformation of $(P_{\text{ss}}, \kappa_{\text{ss}})$ to $R = \mathcal{W}/\mathfrak{m}^k$. If $a, b \in \mathbb{Z}_{p^2}$ satisfy $a^F = -a$ and $b^F = -b$ then the endomorphism*

$$j = \begin{pmatrix} a & \pi b \\ b^F & a^F \end{pmatrix}$$

of P_{ss} lifts to an endomorphism of \tilde{P}_{ss} if and only if

$$k \leq \text{ord}_p(a^2 - b^2\pi) + 1.$$

Proof. The map $R \rightarrow \mathbb{F}_p^{\text{alg}}$ is a PD-thickening by Example 3.6.7. As in Proposition 3.8.2 there is a canonical isomorphism

$$\mathbf{P}_{\text{ss}}(R) \cong P_{\text{ss}} \otimes_{\mathcal{W}} R$$

under which isomorphism the R -module endomorphism

$$\mathbf{j}_R : \mathbf{P}_{\text{ss}}(R) \rightarrow \mathbf{P}_{\text{ss}}(R)$$

is determined by

$$\mathbf{j}_R(x \otimes r) = j(x) \otimes r.$$

The crystal $\mathbf{P}_{\text{ss}}(R)$ is generated as an R -module by $\{e_1 \otimes 1, e_2 \otimes 1\}$. Using the relation

$$\kappa_{\text{ss}}(\varpi) \cdot (e_1 \otimes 1) = (\kappa(\varpi)e_1) \otimes 1 = e_2 \otimes 1$$

we see that $e_1 \otimes 1$ generates $\mathbf{P}_{\text{ss}}(R)$ as an $\mathcal{O}_K \otimes_{\mathbb{Z}} R$ -module. As in the proof Proposition 3.7.4, it follows from Exercise 3.7.2, Exercise 3.7.3, and Lemma 3.7.1 that the unique \mathcal{O}_K -stable lift of the Hodge filtration

$$J_{\mathbb{F}_p^{\text{alg}}} \cdot \mathbf{P}_{\text{ss}}(\mathbb{F}_p^{\text{alg}}) \subset \mathbf{P}_{\text{ss}}(\mathbb{F}_p^{\text{alg}})$$

to $\mathbf{P}_{\text{ss}}(R)$ is

$$J_R \cdot \mathbf{P}_{\text{ss}}(R) \subset \mathbf{P}_{\text{ss}}(R).$$

It follows from Exercise 3.9.2 that $J_R \cdot \mathbf{P}_{\text{ss}}(R)$ is generated as an R -module by

$$(\varpi \otimes 1 - 1 \otimes i(\varpi)) \cdot (e_1 \otimes 1) = e_2 \otimes 1 - e_1 \otimes i(\varpi).$$

This suggests that we define a new R -module basis of $\mathbf{P}_{\text{ss}}(R)$

$$\begin{aligned} f_1 &= e_1 \otimes 1 \\ f_2 &= e_2 \otimes 1 - e_1 \otimes i(\varpi). \end{aligned}$$

The Hodge filtration of the unique deformation of $(P_{\text{ss}}, \kappa_{\text{ss}})$ to R is then

$$(24) \quad Rf_2 \subset Rf_1 \oplus Rf_2.$$

With respect to the basis $\{f_1, f_2\}$ the endomorphism \mathbf{j}_R is given by the matrix

$$\mathbf{j}_R = \begin{pmatrix} a - bi(\varpi) & \pi b - ai(\varpi) \\ -b & -a + bi(\varpi) \end{pmatrix},$$

and in order that \mathbf{j}_R preserve the Hodge filtration (24) we must have

$$\pi b - ai(\varpi) = 0$$

as elements of R . In other words j lifts to an endomorphism of $(\tilde{P}_{\text{ss}}, \tilde{\kappa}_{\text{ss}})$ if and only if

$$\pi b - ai(\varpi) \in \ker(\mathcal{W} \rightarrow R) = i(\varpi^k)\mathcal{W}.$$

This condition is equivalent to

$$\begin{aligned} a - bi(\varpi) \in i(\varpi^{k-1})\mathcal{W} &\iff a^2 - b^2\pi \in p^{k-1}\mathcal{W} \\ &\iff k \leq \text{ord}_p(a^2 - b^2\pi) + 1. \end{aligned}$$

□

Proposition 3.9.4. *Suppose we have a triple $(E, \kappa, j) \in \mathcal{Z}_m(\mathbb{F}_p^{\text{alg}})$ and set*

$$k = \text{ord}_p(m) + 1.$$

The triple (E, κ, j) deforms to $\mathcal{W}/\mathfrak{m}^k$ but not to $\mathcal{W}/\mathfrak{m}^{k+1}$.

Proof. Let (P, κ) be the CM display over $\mathbb{F}_p^{\text{alg}}$ corresponding to (E_{p^∞}, κ) and fix (see Exercise 3.9.1) an isomorphism $(P, \kappa) \cong (P_{\text{ss}}, \kappa_{\text{ss}})$. The endomorphism j corresponds to an endomorphism

$$j = \begin{pmatrix} a & pb \\ b^F & a^F \end{pmatrix}$$

of P_{ss} , and the condition that j be a special endomorphism of (E, κ) is equivalent to the condition

$$a^F = -a \quad b^F = -b.$$

In particular

$$m = j \circ j = \pi b^2 - a^2$$

and so

$$k = \text{ord}_p(m) + 1 = \text{ord}_p(a^2 - \pi b^2) + 1.$$

By Proposition 3.9.3 the triple $(P_{\text{ss}}, \kappa_{\text{ss}}, j)$ deforms to $\mathcal{W}/\mathfrak{m}^k$ but not to $\mathcal{W}/\mathfrak{m}^{k+1}$. By (16) the same is true of (E, κ, j) . □

3.10. Lengths of local rings. As in earlier subsections let p be prime which is nonsplit in K , let \mathfrak{p} be the prime of K above p , and fix $m \in \mathbb{Z}^+$.

Theorem 3.10.1. *Assume that either p is inert in K , or that p is odd and ramified in K . Let $\mathfrak{m} \subset \mathcal{W}$ be the maximal ideal and set*

$$k = e_p \cdot \frac{\text{ord}_p(m) + 1}{2}.$$

For any object R of ART and any $(E, \kappa, j) \in \mathcal{Z}_m(\mathbb{F}_p^{\text{alg}})$ there is a canonical bijection

$$\{\text{deformations of } (E, \kappa, j) \text{ to } R\} \cong \text{Hom}_{\mathcal{W}}(\mathcal{W}/\mathfrak{m}^k, R).$$

Proof. Corollary 3.7.5 implies that for every object R of ART there is a canonical bijection

$$\{\text{deformations of } (E, \kappa) \text{ to } R\} \cong \text{Hom}_{\mathcal{W}}(\mathcal{W}, R)$$

(as both sides consist of a single point!). In other words the deformation functor is pro-represented by \mathcal{W} . It follows from [25, Proposition 2.9] imposing additional endomorphism data in the deformation problem has the effect of passing to a quotient of the pro-representing object. That is to say,

$$\{\text{deformations of } (E, \kappa, j) \text{ to } R\} \cong \text{Hom}_{\mathcal{W}}(\mathcal{W}/I, R)$$

for some ideal $I \subset \mathcal{W}$. This ideal is the smallest ideal for which the triple (E, κ, j) deforms to \mathcal{W}/I , and Propositions 3.8.3 and 3.9.4 tell us that $I = \mathfrak{m}^k$. Indeed, if we take $R = \mathcal{W}/\mathfrak{m}^k$ in the above bijection then the existence of a deformation of (E, κ, j) to $\mathcal{W}/\mathfrak{m}^k$ proves the existence of a \mathcal{W} -algebra map $\mathcal{W}/I \rightarrow \mathcal{W}/\mathfrak{m}^k$. Thus $I \subset \mathfrak{m}^k$. On the other hand if we take $R = \mathcal{W}/\mathfrak{m}^{k+1}$ in the above bijection then the fact that (E, κ, j) does not deform to R implies that there is no \mathcal{W} -algebra map $\mathcal{W}/I \rightarrow \mathcal{W}/\mathfrak{m}^{k+1}$. Thus $I \not\subset \mathfrak{m}^{k+1}$, and we have proved $I = \mathfrak{m}^k$. \square

Theorem 3.10.2 (Gross). *Assume that either p is inert in K , or that p is odd and ramified in K . For every $z \in Z_m(\mathbb{F}_p^{\text{alg}})$ the local ring $\mathcal{O}_{Z_m, z}$ is Artinian of length*

$$\text{length}(\mathcal{O}_{Z_m, z}) = e_p \cdot \frac{\text{ord}_p(m) + 1}{2}.$$

Proof. By combining (13) with Theorem 3.10.1 we see that for every object R of \mathcal{ART} there is a bijection

$$\text{Hom}_{\mathcal{W}}(\widehat{\mathcal{O}}_{Z_m, z}, R) \cong \text{Hom}_{\mathcal{W}}(\mathcal{W}/\mathfrak{m}^k, R).$$

Taking $R = \mathcal{W}/\mathfrak{m}^k$ yields an isomorphism $\widehat{\mathcal{O}}_{Z_m, z} \cong \mathcal{W}/\mathfrak{m}^k$ which shows that $\widehat{\mathcal{O}}_{Z_m, z}$ is Artinian of length k . Using the flatness of the morphism $Z_m \rightarrow Z_m$ it follows that $\widehat{\mathcal{O}}_{Z_m, z}$ is also Artinian of length k . \square

REFERENCES

- [1] B. Conrad. Gross-Zagier revisited. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 67–163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.
- [2] M. Demazure. *Lectures on p -divisible groups*. Springer-Verlag, Berlin, 1972. Lecture Notes in Mathematics, Vol. 302.
- [3] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.
- [4] B. Farb and R. Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.
- [5] B. Gross. On canonical and quasicanonical liftings. *Invent. Math.*, 84(2):321–326, 1986.
- [6] B. Gross and D. Zagier. Heegner points and derivatives of L -series. *Invent. Math.*, 84(2):225–320, 1986.
- [7] A. Grothendieck. *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Les Presses de l'Université de Montréal, Montreal, Que., 1974. Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970).
- [8] H. Hida. *Geometric modular forms and elliptic curves*. World Scientific Publishing Co. Inc., River Edge, NJ, 2000.
- [9] N. Katz. Serre-Tate local moduli. In *Algebraic surfaces (Orsay, 1976–78)*, volume 868 of *Lecture Notes in Math.*, pages 138–202. Springer, Berlin, 1981.
- [10] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.
- [11] S. Kudla. Central derivatives of Eisenstein series and height pairings. *Ann. of Math. (2)*, 146(3):545–646, 1997.
- [12] S. Kudla. Derivatives of Eisenstein series and arithmetic geometry. In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 173–183, Beijing, 2002. Higher Ed. Press.

- [13] S. Kudla. Modular forms and arithmetic geometry. In *Current developments in mathematics, 2002*, pages 135–179. Int. Press, Somerville, MA, 2003.
- [14] S. Kudla. Special cycles and derivatives of Eisenstein series. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 243–270. Cambridge Univ. Press, Cambridge, 2004.
- [15] S. Kudla and M. Rapoport. Arithmetic Hirzebruch-Zagier cycles. *J. Reine Angew. Math.*, 515:155–244, 1999.
- [16] S. Kudla and M. Rapoport. Height pairings on Shimura curves and p -adic uniformization. *Invent. Math.*, 142(1):153–223, 2000.
- [17] S. Kudla and M. Rapoport. Special cycles on unitary Shimura varieties I. Unramified local theory. 2008.
- [18] S. Kudla, M. Rapoport, and T. Yang. On the derivative of an Eisenstein series of weight one. *Int. Math. Res. Not.*, 7:347–385, 1999.
- [19] S. Kudla, M. Rapoport, and T. Yang. Derivatives of Eisenstein series and Faltings heights. *Compos. Math.*, 140(4):887–951, 2004.
- [20] S. Kudla, M. Rapoport, and T. Yang. *Modular forms and special cycles on Shimura curves*, volume 161 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2006.
- [21] W. Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Springer-Verlag, Berlin, 1972. Lecture Notes in Mathematics, Vol. 264.
- [22] W. Messing. Travaux de Zink. *Astérisque*, (311):Exp. No. 964, ix, 341–364, 2007. Séminaire Bourbaki. Vol. 2005/2006.
- [23] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.
- [24] J. Rabinoff. Theory of Witt vectors. *Unpublished notes available online*, 2007.
- [25] M. Rapoport and Th. Zink. *Period spaces for p -divisible groups*, volume 141 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1996.
- [26] K. Ribet. On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
- [27] J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.
- [28] Stephen S. Shatz. Group schemes, formal groups, and p -divisible groups. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 29–78. Springer, New York, 1986.
- [29] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971.
- [30] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
- [31] J. Tate. p -divisible groups.. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.
- [32] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.
- [33] T. Zink. The display of a formal p -divisible group. *Astérisque*, (278):127–248, 2002. Cohomologies p -adiques et applications arithmétiques, I.