On the Hasse–Witt Invariants of Modular Curves

Pilar Bayer and Josep González

CONTENTS

This research has been partially supported by DGICYT, PB-93-0034.

We briefly discuss the relationship between several characterizations of the Hasse–Witt invariant of curves in characteristic p with the goal of computing its value in concrete instances. We study its asymptotic behaviour when dealing with the geometric fibres of curves of genus ≥ 2 defined over the rationals. Numerical evidence gathered for several modular curves supports certain conjectural distribution laws.

1. INTRODUCTION

Throughout, we assume that k is an algebraically closed field of characteristic $p > 0$, and $\mathcal{C}/k$ denotes a complete nonsingular curve of genus $g > 0$. We know [Hasse 1934; Hasse and Witt 1936] that the number $r(\mathcal{C})$ of maximal independent unramified $\mathbb{Z}/p\mathbb{Z}$-extensions of the function field $k(\mathcal{C})$ satisfies the inequalities $0 \leq r(\mathcal{C}) \leq g$. It is said that the integer $r = r(\mathcal{C})$ is the Hasse–Witt invariant of $\mathcal{C}$.

If $\mathcal{C}$ is elliptic, the only possible values for r are 1 or 0. If $r = 1$, the curve is said to be ordinary; otherwise, it is said to be supersingular. If $\mathcal{C}/\mathbb{Q}$ is an elliptic curve with complex multiplication, the set of supersingular primes for $\mathcal{C}$ has density equal to $\frac{1}{2}$ [Deuring 1941] (compare [de Shalit 1987]). If $\mathcal{C}/\mathbb{Q}$ is an elliptic curve that does not have complex multiplication, the set of supersingular primes has density equal to zero [Serre 1981]. Elkies [1987] proved that this set is infinite. Lang and Trotter [1976] conjectured that

$$P_{\mathcal{C}}(x) \sim c\sqrt{x}/\log x \quad \text{ as } x \to \infty,$$

where $P_{\mathcal{C}}(x)$ denotes the number of supersingular primes for $\mathcal{C}$ that are $\leq x$ and $c > 0$ is a constant depending on $\mathcal{C}$. It has been proved by Elkies and Murty that $P_{\mathcal{C}}(x) = O(x^{3/4})$ [Elkies 1991].

1058-6458/97 \$0.50 per page

Let J/k be the jacobian of $\mathcal{C}/k$, and $J[p]$ the kernel of the multiplication by p in $J(k)$. We have the equality $r(\mathcal{C}) = \dim_{\mathbb{F}_p} J[p]$. Accordingly, for any given abelian variety A/k, we let

$$r(A) := \dim_{\mathbb{F}_p} A[p],$$

and call this integer the Hasse–Witt invariant of A. It then follows that $0 \leq r(A) \leq \dim A$. Ordinary abelian varieties are those for which $r(A) = \dim A$. If A is isogenous to a product $\prod A_i$ of abelian varieties, then $r(A) = \sum r(A_i)$.

The behaviour of the Hasse–Witt invariant for the geometric fibres of abelian varieties $A/\mathbb{Q}$ of dimension ≥ 2 is less well known. We study its variation with p. If p is a prime of good reduction for A, we let $r_p(A) := r(A_{/\bar{\mathbb{F}}_p})$, and prove that there are infinitely many primes for which $r_p(A) \geq 2$. However, at present, given an abelian variety $A/\mathbb{Q}$ of dimension > 2, it is not known whether the set of primes of ordinary reduction is always infinite.

Let $P_A(x)$ denote the number of nonordinary primes for $A/\mathbb{Q}$ that are $\leq x$. Let $P_{A,0}(x)$ denote the number of primes $p \leq x$ for which $r_p(A) = 0$. The size of $P_A(x)$ and $P_{A,0}(x)$ seems to depend on phenomena of real, complex, and quaternionic multiplication. Cases arising from the Fermat curves were treated in [González 1997]. In this paper we deal with cases that arise from modular curves, and formulate a higher-dimensional analogue of the Lang and Trotter conjecture.

Let Γ denote a congruence subgroup, f a newform of weight two for Γ, and $A_f/\mathbb{Q}$ the abelian variety attached to f by Shimura's construction. The set of primes p for which $r_p(A_f) = 0$ and $A_{f/\bar{\mathbb{F}}_p}$ is not isogenous to a power of a supersingular elliptic curve is finite. Suppose that f does not have complex multiplication. Then the set of primes p for which $r_p(A_f) = 0$ has density equal to zero. As is well known, A_f is isogenous to a power of a $\bar{\mathbb{Q}}$-simple abelian variety B_f of dimension td, where $t = 1$ or 2, and $t = 1$ if and only if the endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}(B_f)$ is commutative. Numerical computations performed in the range of levels up to one hundred and primes $p \leq 10^4$ lead us to conjecture the following asymptotic relations, where $c_f, c_{f,0}$ are positive constants and $c_f = c_{f,0}$ for $d = 1$:

(i) If $d = 1$, $P_{A_f}(x) \sim c_f \sqrt{x}/\log x$ as $x \to \infty$.
(ii) If $d \geq 2$, $P_{A_f}(x) \sim c_f \log\log x$ as $x \to \infty$.
(iii) If $d = 1$, $P_{A_{f,0}}(x) \sim c_{f,0} \sqrt{x}/\log x$ as $x \to \infty$.
(iv) If $d = 2$, $P_{A_{f,0}}(x) \sim c_{f,0} \log\log x$ as $x \to \infty$.
(v) If $d > 2$, $P_{A_{f,0}}(x) = O(1)$ for all $x \geq 2$.

We also construct a probabilistic model that predicts these behaviours.

2. SOME FACTS ON SEMILINEAR ALGEBRA

In this section we consider some facts on semilinear algebra. We fix an integer n, a power $q = p^n$ of the characteristic of k, and H, H_i denote k-vector spaces.

Definition 2.1. An additive mapping $F : H_1 \to H_2$ is said to be *q-linear* if it satisfies $F(\lambda x) = \lambda^q F(x)$ for all $\lambda \in k$ and $x \in H_1$.

By $\mathrm{End}_q(H)$ we denote the k-vector space of all q-linear operators on H. In the linear case, $n = 0$, we simply drop the subindex q. For a given matrix M with entries in k, $M^{(q^i)}$ will denote the matrix obtained from M by raising each of its entries to the q^i-th power. If we choose a basis of H, then we may attach to any q-linear operator F on H a matrix W in the usual way: if $x = (x_i)$ denotes a vector of H, then $Wx^{(q)}$ yields the coordinates of the vector $F(x)$. Note that, for any integer $m > 0$, F^m is a q^m-linear operator with matrix $W(m) := WW^{(q)} \cdots W^{(q^{m-1})}$.

If $F \in \mathrm{End}_q(H)$, the dual operator F' is defined by $(F'(\omega)(e))^q = \omega(F(e))$, for any form ω in the dual linear space H' and any vector $e \in H$. Then $F' \in \mathrm{End}_{q^{-1}}(H')$ and, if W is the matrix of F in the basis $\{e_1, \dots, e_g\}$, the matrix W' of F' in the dual basis is given by $W' = (W^t)^{(1/q)}$, where W^t denotes the transposed matrix.

The q-linear nonlinear operators do not have attached eigenvalues or characteristic polynomials.

Each operator F yields a decomposition $H = H_s \oplus H_n$ into invariant subspaces, where F restricted to H_s is semisimple and restricted to H_n is nilpotent. We consider

$$r(F) := \dim H_s,$$
$$s_i(F) := \dim \ker F^i \quad \text{for } 1 \le i \le g,$$

where $g = \dim H$. The integer $r(F)$ is called the semisimple rank of F. The integers $s_i(F)$ determine $r(F)$ and the number and length of the Jordan boxes of the H_s; they remain invariant by changes of basis. In particular,

$$r(F) = \dim \operatorname{im} F^g = \operatorname{rank} W(g) = g - s_g(F).$$

Moreover, $r(F) = \dim_{\mathbb{F}_{q'}} H^F$, where q' is the maximum between q and q^{-1}. Observe that F and F' have the same invariants.

Given $F \in \operatorname{End}_q(H)$, and any basis $\{e_1, \dots, e_g\}$ of H, we may consider the linear operator $T \in \operatorname{End}(H)$ defined by $T(e_i) = F(e_i)$ for $1 \le i \le g$. Although $\dim \ker F = \dim \ker T$, it might happen that $\dim \ker F^m$ and $\dim \ker T^m$ do not agree. The following definition is useful for our purposes.

Definition 2.2. We say that a linear operator $T \in \operatorname{End}(H)$ *strongly linealizes* a q-linear operator $F \in \operatorname{End}_q(H)$ if there exists a basis $\{e_1, \dots, e_g\}$ of H such that for any integer $j > 0$ is

$$T^j(e_i) = F^j(e_i) \quad \text{for } 1 \le i \le g.$$

A linear operator T *linealizes* a q-linear operator F if some power of T strongly linealizes some (possibly different) power of F.

Clearly, if $F \in \operatorname{End}_q(H)$ is such that in some basis it has a matrix W with entries in $\mathbb{F}_q$, $q > 1$, and if $T \in \operatorname{End}(H)$ is the linear mapping defined through W, then T strongly linealizes F. If T linealizes F, then the semisimple rank of F equals the sum of the multiplicities of the nonzero roots of the characteristic polynomial of T, since the dimensions of the nilpotent subspaces attached to F and T are the same.

Proposition 2.3. *If $k = \bar{\mathbb{F}}_q$ and $T \in \operatorname{End}(H)$ is an operator that linealizes $F \in \operatorname{End}_q(H)$, then the dual operator T' linealizes the dual operator F'.*

3. HASSE–WITT INVARIANT OF ABELIAN VARIETIES OVER FINITE FIELDS

Let A/k be an abelian variety of dimension g. We denote by F_A^* the p-linear operator of $H^1(A, \mathcal{O})$ induced by the absolute Frobenius F_A, and by C_A the Cartier operator of $H^0(A, \Omega^1)$, which is p^{-1}-linear. As is well known, $r(A) = r(F_A^*)$.

Let $(\hat{A}/k, \mathcal{P}_A)$ be the dual abelian variety of A, where $\hat{A}(k) = \operatorname{Pic}^0(A)$ and $\mathcal{P}_A$ is the Poincaré sheaf over $A \times \hat{A}$. Let $T_0(-)$ denote tangent space at zero. By considering the canonical isomorphism $\mu : T_0(\hat{A}) \to H^1(A, \mathcal{O})$, we get a canonical pairing

$$H^1(A, \mathcal{O}) \times H^0(\hat{A}, \Omega^1) \to k, \quad \langle r, \widehat{\omega} \rangle := \widehat{\omega}(\mu^{-1}(r))$$

for which the dual operator of the absolute Frobenius F_A^* is the Cartier operator $C_{\hat{A}}$. Moreover, $\langle \psi^* r, \widehat{\omega} \rangle = \langle r, \widehat{\psi}^*(\widehat{\omega}) \rangle$ for any $\psi \in \operatorname{End}(A)$.

Until the end of this section, we assume that A is defined over $\mathbb{F}_q$, $q = p^n$, and $k = \bar{\mathbb{F}}_q$. Let $\varphi \in \operatorname{End}_{\mathbb{F}_q}(A)$ denote the relative Frobenius endomorphism of A. For each prime $l \ne p$, let $T_l(A)$ be the l-adic Tate module, and $V_l(A) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(A)$.

Proposition 3.1. (i) *The linear operator*

$$\varphi^* : H^1(A, \mathcal{O}) \to H^1(A, \mathcal{O})$$

linealizes the p-linear operator F_A^*.

(ii) *The Hasse–Witt invariant of A is the sum of the multiplicities of the nonzero roots of the* $\bmod p$ *reduced characteristic polynomial of φ acting on $V_l(A)$.*

Proof. The assertion in (i) follows from the fact that for any $r \in H^1(A, \mathcal{O})$ there exists an integer $m_r > 0$ such that if $m_r \mid m$, then $(\varphi^*)^m(r) = (F^*)^{nm}(r)$. The assertion in (ii) follows from (i) combined with

$$\det(\varphi - x \operatorname{Id} \mid V_l(A)) \pmod p = (-1)^g x^g \det(\varphi^* - x \operatorname{Id} \mid H^1(A, \mathcal{O})),$$

due to Manin [1961]. $\square$

Consider an $\mathbb{F}_q$-polarization $\lambda : A \to \hat{A}$ and the corresponding Rosati involution in $\mathbb{Q}\otimes\mathrm{End}(A)$ defined by $\psi \mapsto \psi' = \lambda^{-1}\circ\widehat{\psi}\circ\lambda$. Note that the *Verschiebung* φ' lies in $\mathrm{End}_{\mathbb{F}_q}(A)$. Since $\varphi_A\circ\varphi'_A = q$ and $\varphi_A\circ\hat{\varphi}_{\hat{A}} = q$, we have that the Verschiebung endomorphism of A is $\hat{\varphi}_{\hat{A}}$; that is, $\varphi'_A = \hat{\varphi}_{\hat{A}}$. Thus, ${\varphi_{\hat{A}}}^*$ and ${\varphi'}^*_A$ are dual with respect to the above pairing. Since the respective Frobenius acting on $V_l(A), V_l(\hat{A})$ have the same characteristic polynomial, we get

Proposition 3.2. (i) *The linear operator*

$$\varphi'^* : H^0(A,\Omega^1)\to H^0(A,\Omega^1)$$

linealizes the p^{-1}-linear operator C_A. Thus the Hasse–Witt invariant of A is the sum of the multiplicities of the nonzero roots of the characteristic polynomial of φ'^* acting on $H^0(A,\Omega^1)$.

(ii) *The characteristic polynomial of φ^* acting on $H^1(A,\mathcal{O})$ equals the characteristic polynomial of φ'^* acting on $H^0(A,\Omega^1)$.*

Let $P(x) := \det(\varphi - x\,\mathrm{Id}\mid V_l(A))$. As is well known, $P(x)$ is a polynomial with integral coefficients, independent of l. If α_i, $1\le i\le 2g$, denote its complex roots, we have $|\alpha_i| = q^{1/2}$, $\prod_{i=1}^{2g}\alpha_i = q^g$, and we may fix an ordering of the roots of $P(x)$ so that $\alpha_{i+g} = \overline{\alpha_i} = q/\alpha_i$ for $1\le i\le g$. Let $\beta_i := \alpha_i + \bar{\alpha}_i$, $1\le i\le g$. The polynomial $Q(x) := \prod_{i=1}^{g}(x-\beta_i)$ has integral coefficients and $Q(x)^2 = \det(\varphi+\varphi' - x\,\mathrm{Id}\mid V_l(A))$. We have $\det(\varphi - x\,\mathrm{Id}\mid V_l(A)) \equiv x^g Q(x) \pmod{p}$. Thus $r(A)$ equals the sum of the multiplicities of the nonzero roots of $Q(x) \pmod{p}$, and

$$\begin{aligned}\det(\varphi^* - x\,\mathrm{Id}\mid H^1(A,\mathcal{O})) &= \det(\varphi'^* - x\,\mathrm{Id}\mid H^0(A,\Omega^1))\\ &= (-1)^g Q(x) \pmod{p}.\end{aligned}$$

4. HASSE–WITT INVARIANTS OF MODULAR CURVES

Let $N>1$ be an integer and Γ a subgroup of $\Gamma_0(N)$ containing $\Gamma_1(N)$. Denote by X_Γ the complex projective nonsingular curve defined by the action of Γ in the completed upper-half plane $\mathbb{H}^*$. If $N>4$, the curve X_Γ has a proper and smooth model over $\mathbb{Z}[1/N]$. The Hecke and the diamond correspondences $[T_p]$ and $\langle p\rangle$, for $p\nmid N$ a prime, act on it. The Weil involution w is an automorphism of X_Γ defined over $\mathbb{Z}[1/N][\zeta]$, where ζ is a primitive N-th root of unity.

From now on we consider only modular curves of genus $g>0$. We fix a prime $p\nmid N$, and a place $\bar{p}$ of $\overline{\mathbb{Q}}$ lying over p. We let $\mathfrak{J}_\Gamma/\operatorname{Spec}\mathbb{Z}_p[\zeta]$ be the Néron model of the jacobian of $X_\Gamma/\operatorname{Spec}\mathbb{Z}_p[\zeta]$. We denote by $\tilde{X}_p = X_{\Gamma/\bar{\mathbb{F}}_p}$, $\tilde{J}_p = \mathfrak{J}_{\Gamma/\bar{\mathbb{F}}_p}$ the corresponding geometric closed fibres. For any endomorphism ψ of $\mathfrak{J}_\Gamma$, we let $\tilde{\psi}$ denote its $\bmod\,\bar{p}$ reduction.

Let T_p be the p-th Hecke operator acting on the space of cusp forms $S_2(\Gamma)$. Under the isomorphism $S_2(\Gamma)\to H^0(X_\Gamma,\Omega^1)$ given by $f(q)\mapsto f(q)q^{-1}dq$, the T_p operator induced on $H^0(X_\Gamma,\Omega^1)$ equals $(\iota^*)^{-1}[T_p]^*\iota^*$. Here $q = e^{2\pi i z}$, and ι denotes a canonical mapping from the modular curve to its jacobian.

Proposition 4.1. *The endomorphism $\widetilde{[T_p]}^*$ of the vector space $H^0(\tilde{J}_p,\Omega^1)$ equals $(\tilde{w}^{-1}\circ\varphi'\circ\tilde{w})^*$. The Hasse–Witt invariant of $\tilde{X}_p$ is the sum of the multiplicities of the nonzero roots of the $\bmod\,p$ reduced characteristic polynomial $\det(T_p - x\,\mathrm{Id}\mid S_2(\Gamma))$.*

Proof. Eichler–Shimura congruence [Shimura 1971] tells us

$$\widetilde{[T_p]} = \varphi + \varphi'\circ\widetilde{\langle p\rangle} = \varphi + \tilde{w}^{-1}\circ\varphi'\circ\tilde{w},$$

as equality in $\mathrm{End}(\tilde{J}_p)$. Since $\varphi^* = 0$ on $H^0(\tilde{J}_p,\Omega^1)$, the first statement follows. The rest is a consequence of proposition 3.2(ii) combined with the following equalities and congruence $\bmod\,p$:

$$\begin{aligned}&\det(T_p - x\,\mathrm{Id}\mid S_2(\Gamma))\\ &\qquad = \det([T_p]^* - x\,\mathrm{Id}\mid H^0(J_\Gamma,\Omega^1))\\ &\qquad \equiv \det(\widetilde{[T_p]}^* - x\,\mathrm{Id}\mid H^0(\tilde{J}_\Gamma,\Omega^1))\\ &\qquad = \det(\varphi'^* - x\,\mathrm{Id}\mid H^0(\tilde{J}_\Gamma,\Omega^1)).\quad\square\end{aligned}$$

Proposition 4.2. *Let ε denote a $\bmod\,N$ Dirichlet character and $f = \sum_{n>0}a(n)q^n$ in $S_2(\Gamma_0(N),\varepsilon)$ a modular form whose coefficients belong to the integer ring $\mathcal{O}_E$ of a number field E. Let $\mathfrak{p}$ be a prime* *ideal of $\mathcal{O}_E$ over p of residue degree equal to ν. Then, for each integer $m > 0$ such that $\nu \mid m$, we have*

$$\widetilde{T_p}^{m}(\widetilde{f(q)q^{-1}dq}) = C^m(\widetilde{f(q)q^{-1}dq}),$$

where $\tilde{}$ *denotes reduction* $\bmod \bar{p}$.

Proof. We recall that for any curve $\mathcal{C}/k$ in characteristic $p > 0$, the Cartier operator C is defined in the following way: given a closed point x in $\mathcal{C}$ and functions $t, h \in \mathcal{O}_x$ such that $dt \neq 0$, then $C(hdt) = h_1 dt$, where $h_1^p = -d^{p-1}h/dt^{p-1}$. The claim of the proposition follows by considering $\mathcal{C} = \tilde{X}_p$, $x = i\infty$, and $t = q$. □

We see that the Cartier operator and the Hecke operator $\tilde{T}_p$ agree on the $\bmod p$ reduced parabolic forms of $S_2(\Gamma_0(N), \varepsilon)$ whose coefficients lie in $\mathbb{Z}$. In the particular case of the trivial Nebentypus character, $S_2(\Gamma_0(N))$ has a basis of parabolic forms with integral coefficients, hence the two operators agree on the $\bmod p$ reduced basis. On the other hand, since $S_2(\Gamma_0(N), \varepsilon)$ has a basis of eigenfunctions of the T_p-operator with algebraic integral coefficients, we get

Corollary 4.3. *The Hecke operator $\widetilde{[T_p]}^*$ of $H^0(\tilde{J}_p, \Omega^1)$ linealizes the Cartier operator C. If $\Gamma = \Gamma_0(N)$, then $\widetilde{[T_p]}^*$ strongly linealizes C.*

Numerical calculations of Hasse–Witt invariants of modular curves will be displayed in Section 9. They have been performed by using proposition 4.1 and the available tables for the characteristic polynomials of the Hecke operators. If $X_0(N)$ happens to be hyperelliptic, we may compute a matrix for the Cartier operator at $p \nmid 2N$ by the method of [Manin 1962], which in turn requires the knowledge of an equation of the curve. If we use for that purpose the equations in [Gonzàlez Rovira 1991], then the characteristic polynomial of that matrix equals the $\bmod p$ reduced characteristic polynomial of T_p. This happens because the basis of regular differentials obtained from those equations corresponds to modular forms that do have integral Fourier coefficients.

5. SOME RESULTS ON DENSITIES

From now on, A will denote an abelian variety defined over $\mathbb{Q}$ and p a prime of good reduction for A. We write $\tilde{A}_p = A_{/\bar{\mathbb{F}}_p}$, and $r_p(A) := r(\tilde{A}_p)$. We say that p is a prime of ordinary reduction for A if $r_p(A) = \dim A$. If $\dim A = 1$, we already mentioned the existence of infinitely many primes of ordinary reduction as well as of supersingular reduction. In higher dimensions, we find the following result.

Proposition 5.1. *Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 2$. Then, there exists a set of primes with positive density for which $r_p(A) \geq 2$ for all p in this set. In particular, if $g = 2$, there exists a set of primes of ordinary reduction for A that has positive density.*

Proof. Let us fix a prime $l > 4g^2$ and let p be a prime of good reduction for A such that it splits completely in the field $\mathbb{Q}(A[l])$. Since $\mathbb{Q}(\mu_l) \subseteq \mathbb{Q}(A[l])$, then $p \equiv 1 \pmod{l}$ and, in particular, $p > l$ and the points in $\tilde{A}_p[l]$ are rational over $\mathbb{F}_p$. Thus, the relative Frobenius φ_p acts trivially on $\tilde{A}_p[l]$. Since $p \equiv 1 \pmod{l}$, the Verschiebung $\varphi_p' = p/\varphi_p$ also acts trivially on $\tilde{A}_p[l]$. If we consider $\varphi_p + \varphi_p'$ acting on $T_l(\tilde{A}_p)$, we have $\varphi_p + \varphi_p' \equiv 2\,\mathrm{Id} \pmod{l}$. If $Q(x) = x^g + \sum_{i=1}^{g-1} c_i x^{g-i}$ is the polynomial with integral coefficients such that $Q(x)^2 = \det(\varphi_p + \varphi_p' - x\,\mathrm{Id} \mid V_l(\tilde{A}_p))$ (cf. section 3), then

$$x^g + \sum_{i=1}^{g-1} c_i x^{g-i} \equiv (x-2)^g \pmod{l}.$$

From this we get $c_1 \equiv -2g \pmod{l}$ and $c_2 \equiv 2g(g-1) \pmod{l}$. On the other hand, we know that $|c_1| \leq 2gp^{1/2} < p$ and $|c_2| \leq 2g(g-1)p < lp$. For such primes p we must have $r_p(A) > 0$, since the condition $c_1 \equiv 0 \pmod{p}$ would imply $c_1 = 0$, which contradicts the fact that $c_1 \equiv -2g \pmod{l}$. We claim that $c_2 \not\equiv 0 \pmod{p}$, which already implies $r_p(A) > 1$. Assume instead that $c_2 \equiv 0 \pmod{p}$, then $c_2 = 2g(g-1)p$. Since all the roots of the polynomial $Q(x)$ are real, then all the roots of the

i-th derived polynomials $Q^{(i)}(x)$, for $1 \leq i \leq g-1$, are also real. Therefore, the roots of the polynomial

$$\frac{2Q^{g-2)}(x)}{g!} = x^2 + 2\frac{c_1}{g}x + 4p$$

are real, so that $c_1^2 \geq 4g^2 p$. Since $|c_1| \leq 2gp^{1/2}$, we get $|c_1| = 2gp^{1/2}$, which contradicts the fact that c_1 is an integer. □

Another proof, due to Ogus, of the second claim of the preceding proposition can be found in [Deligne et al. 1982].

Next we work on abelian subvarieties $A/\mathbb{Q}$ of the jacobian of the modular curve $X_\Gamma/\mathbb{Q}$. Let $f = \sum_{n>0} a(n)q^n \in S_2(\Gamma)$ be a newform, E the field generated by its coefficients and I the set of $\mathbb{Q}$-embeddings of E into $\bar{\mathbb{Q}}$. Let $A_f/\mathbb{Q}$ denote the abelian subvariety of J_Γ of dimension $g = [E:\mathbb{Q}]$ whose cotangent vector space, H_f, is generated by $\{f^\sigma\}$ for σ running into I (compare [Shimura 1971]). H_f has a basis of modular forms with integral Fourier coefficients. From what we have seen, $r_p(A_f)$ equals the sum of the multiplicities of the nonzero roots of the mod p reduced polynomial $\det(T_p - x\,\mathrm{Id} \mid H_f)$. Therefore,

$$r_p(A_f) = \#\{\sigma \in I \mid a(p)^\sigma \not\equiv 0 \pmod{\bar{p}}\}.$$

In particular, A_f is ordinary at p if and only if $p \nmid N_{E/\mathbb{Q}}(a(p))$. If f has complex multiplication [Ribet 1977], it follows that there is a set of primes p with density $1/2$ for which $r_p(A_f) = 0$.

Proposition 5.2. *Suppose that $A/\mathbb{Q}$ is an abelian subvariety of J_Γ that is invariant under all the Hecke endomorphisms.*

(i) *For almost all primes p, $r_p(A) = 0$ implies*

$$[T_p]_{|A} = 0.$$

(ii) *If $[T_p]_{|A} = 0$, then $\tilde{A}_p$ is $\bar{\mathbb{F}}_p$-isogenous to a power of a supersingular elliptic curve. Hence, the set of primes for which is $r_p(A) = 0$ and $\tilde{A}_p$ is not $\bar{\mathbb{F}}_p$-isogenous to a power of a supersingular elliptic curve is finite.*

(iii) *If the cotangent space to A does not contain any form with complex multiplication, then the set of primes p for which $r_p(A) = 0$ has natural density, in the set of all primes numbers, equal to zero.*

Proof. Without loss of generality, we may assume that $A = A_f$ is the variety attached to a newform $f \in S_2(\Gamma)$. Let $\{f_1, \dots, f_g\}$ be a basis of newforms and $\{h_1, \dots, h_g\}$ a basis of forms with integral coefficients of H_f. Let $M = (m_{ij})$ be the matrix of the change of basis, so that $h_j = \sum_i m_{ij} f_i$. Let c denote an upper bound of the values $|m_{ij}|$, and let $\mathcal{Q}$ denote the set of primes such that m_{ij} is p-integral, $p \nmid N$, and $p^{1/2} > 2gc$. If $f_i = \sum_{n>0} a_i(n)q^n$, $h_i = \sum_{n>0} c_i(n)q^n$, then we get

$$|c_j(p)| = \Bigl|\sum m_{ij}a_i(p)\Bigr| \leq c\sum |a_i(p)| < c2gp^{1/2} < p$$

for all $p \in \mathcal{Q}$. Assume now that $r_p(A_f) = 0$. If the entries in the matrix M are p-integral, we must have $c_i(p) \equiv 0 \pmod{p}$ for $1 \leq i \leq g$. If $p \in \mathcal{Q}$, we therefore get $c_i(p) = 0$. Since $\det M \neq 0$, $a_i(p) = 0$ for $1 \leq i \leq g$. We see that $T_p = 0$ on H_f. This yields statement (i).

By Eichler–Shimura, $[\tilde{T}_p] = \varphi_p + \varphi_p'\widetilde{\langle p\rangle} = \varphi_p + p/\varphi_p\widetilde{\langle p\rangle}$. Hence, if we now assume that $[T_p]_{|A} = 0$, a power of φ_p will be equal to the multiplication by an integer. Since $\tilde{A}_p$ is defined over a finite field, we know [Tate 1966] that this condition is equivalent to $\tilde{A}_p$ being isogenous to a power of a supersingular elliptic curve. This yields statement (ii).

For a form f without complex multiplication, it was proved by Serre [1981] that the number $P_{f,0}(x)$ of primes $p \leq x$ such that $a(p) = 0$ satisfies

$$P_{f,0}(x) = O\biggl(\frac{(\log\log\log x)^{1/2}}{(\log x)^{1/2}}\log\log x\,\mathrm{Li}(x)\biggr)$$

as $x \to \infty$. From this formula, statement (i), and the prime number theorem, we get statement (iii). □

6. FROBENIUS DISTRIBUTIONS: FIRST APPROACH

Throughout the remainder of the paper,

$$f = \sum_{n>0} a(n)q^n \in S_2(N, \varepsilon)$$

denotes a newform without complex multiplication, $g = \dim A_f$, $\mathcal{O}_E$ the ring of integers of the number field E generated by the coefficients of f, and $I = \{\sigma_1, \dots, \sigma_g\}$ the set of all $\bar{\mathbb{Q}}$-embeddings of E into $\bar{\mathbb{Q}}$. We let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

For each prime l, we know that there exists a continuous l-adic representation

$$\rho_l : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathcal{O}_E \otimes \mathbb{Z}_l)$$

unramified outside Nl and such that

$$\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p})) = a(p),$$
$$\det(\rho_l(\mathrm{Frob}_{l,p})) = \varepsilon(p)p$$

for all primes $p \nmid Nl$. Here $\mathrm{Frob}_{l,p} = \mathrm{Frob}_{l,p}(M_l/\mathbb{Q})$ denotes a Frobenius element and M_l is the Galois extension of $\mathbb{Q}$ cut out by ρ_l. The family ρ_l, for all primes l, defines an homomorphism

$$\rho : G_{\mathbb{Q}} \to \prod_l \mathrm{GL}(2, \mathcal{O}_E \otimes \mathbb{Z}_l).$$

Let T be the set of those pairs (σ, χ) such that $\sigma \in I$ and $\chi : G_{\mathbb{Q}} \to \mathbb{C}^*$ is a continuous character that satisfies $a(p)^\sigma = \chi(p)a(p)$ for all $p \nmid N$. The set $T \neq \varnothing$ is a group by the law

$$(\tau, \psi) \cdot (\sigma, \chi) = (\tau \circ \sigma,\ \chi^\tau.\psi),$$

where $\chi^\tau(g) := \chi(g)^\tau$. If $(\sigma, \chi) \in T$, then χ is unramified outside N and $\chi = \mu\varepsilon^j$ with some character μ of order 1 or 2 and some integer j. Let Γ be the subset of the elements $\sigma \in I$ such that $(\sigma, \chi) \in T$ for some χ. It turns out that Γ is an abelian subgroup of the group of automorphisms of E. Let $\Delta = \bigcap \ker \chi$ for $(\sigma, \chi) \in T$. Consider the number fields

$$L = \bar{\mathbb{Q}}^{\Delta}, \quad F = E^{\Gamma}.$$

We will now record some facts concerning these fields L and F that are needed in the sequel. For their proofs see [Momose 1981; Ribet 1980; 1985; 1992; 1994].

(i) The extension $L/\mathbb{Q}$ is abelian and the number field F is totally real.
(ii) The mapping $T \to \Gamma = \mathrm{Gal}(E/F)$ given by $(\sigma, \chi) \mapsto \sigma$ is an isomorphism.
(iii) Replacing each ρ_l by an isomorphic representation, we may suppose that $\rho_l(\Delta)$ is contained in the subgroup $\{s \in \mathrm{GL}(2, \mathcal{O}_F \otimes \mathbb{Z}_l) \mid \det s \in \mathbb{Z}_l^*\}$, and that it is equal to it for almost all l.
(iv) For each prime $p \nmid N$, we have $a(p)^2/\varepsilon(p) \in F$.
(v) The abelian variety A_f is isotypical; i.e., $\overline{\mathbb{Q}}$-isogenous to a product $B \times \cdots \times B$, where $B = B_f$ is a $\bar{\mathbb{Q}}$-simple abelian variety. The endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}(B_f)$ is a central division algebra over F of dimension t^2, with $t \leq 2$. Moreover, $\dim B_f = td$, where $d = [F : \mathbb{Q}]$.

The following relationship between the fields L and F, although elementary, will be basic for predicting the distribution laws of the $a(p)$-s values. Note that if A_f is an elliptic curve, then both fields are equal and coincide with $\mathbb{Q}$.

Main Lemma 6.1. *Assume that for a prime $p \nmid N$, the geometric fibre $\tilde{A}_{f,p}$ is not isogenous to a power of a supersingular elliptic curve. Let κ denote the residue degree of any prime in L over p. For a given integer m, the following conditions are equivalent*:

(a) $a(p)^m \in \mathcal{O}_F$,
(b) $\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p}^m)) \in \mathcal{O}_F \otimes \mathbb{Z}_l$ *for all* $l \neq p$,
(c) $\kappa \mid m$.

Proof. The hypothesis over $\tilde{A}_{f,p}$ implies, as in the proof of 5.2, that $\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p}^m)) \neq 0$ for all $l \neq p$, and $m > 0$. We first show the equivalence of (a) and (b). For a given 2×2-matrix s with entries in an integral domain, and for any $m > 0$, the following identity is fulfilled:

$$\mathrm{Tr}(s^m) = \sum_{i=0}^{[m/2]} (-1)^i \frac{m}{m-i} \binom{m-i}{i} (\det s)^i (\mathrm{Tr}\, s)^{m-2i}.$$

Thus, under the assumption $\mathrm{Tr}(s) \neq 0$, we have

$$\mathrm{Tr}(s^m) = (\mathrm{Tr}\, s)^m \left(\sum_{i=0}^{[m/2]} (-1)^i \frac{m}{m-i} \binom{m-i}{i} \left(\frac{\det s}{(\mathrm{Tr}\, s)^2} \right)^i \right).$$

Since $\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p}^m)) \neq 0$ for all $m > 0$, we have $a(p)^m \in F$ if and only if, for each $l \neq p$, we have $\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p}^m)) \in \mathcal{O}_F \otimes \mathbb{Z}_l$, due to the fact that $a(p)^2/\varepsilon(p) \in F^*$.

We now show that (c) implies (b). Since $p \nmid N$, p is unramified in L. For a place $\bar{p}$ of $\bar{\mathbb{Q}}$ over p, let $\mathfrak{p}$ be its restricion to L. Since $\mathrm{Frob}_{l,p}(M_l L/\mathbb{Q})^\kappa = \mathrm{Frob}_{l,\mathfrak{p}}(M_l L/L)$ and by taking into account c), we get $\mathrm{Tr}(\rho_l(\mathrm{Frob}_{l,p}^\kappa)^{m/\kappa}) \in \mathcal{O}_F \otimes \mathbb{Z}_l$.

Finally, we show that (a) implies (c). If $a(p)^m \in F$, then for all $(\sigma, \chi) \in T$ we have $(a(p)^m)^\sigma = a(p)^m$. Since $a(p) \neq 0$, we have $\chi(p^m) = 1$, so that $\chi(\mathrm{Frob}_{l,p}(M_l L/\mathbb{Q})^m) = \chi(p^m) = 1$. Therefore, $\mathrm{Frob}_{l,p}(M_l L/\mathbb{Q})^m \in \mathrm{Gal}(M_l L/L)$ and $\kappa \mid m$. □

Since A_f is isogenous to a power of B_f, we have

$$r_p(A_f) = r(B_{f/\mathbb{F}_p}) \dim A_f / \dim B_f.$$

Hence, the Hasse–Witt invariants of A_f are determined by those of the geometric fibres of its building block B_f.

Throughout the remainder of the paper, $\mathcal{P} = \mathcal{P}_L$ will denote the set of primes $p \nmid N$ that split completely in L. If $p \in \mathcal{P}_L$, we know by 6.1 that $a(p) \in F$. In this case we let $b(p) := N_{F/\mathbb{Q}}(a(p))$. By Section 5, A_f is nonordinary at p if and only if $b(p) \equiv 0 \pmod p$, and $r_p(A_f) = 0$ if and only if $b(p) = 0$ for large enough p.

In general, $|N_{E/\mathbb{Q}}(a(p))| \leq 2^g p^{g/2}$, but for $p \in \mathcal{P}_L$ we have $|b(p)| \leq 2^d p^{d/2}$. Moreover, for the primes $p \notin \mathcal{P}_L$, the values $a(p)$ are constrained by the condition $a(p)^\kappa \in F$. These facts lead us to suspect that the pair L, F might control the distribution law of the nonordinary primes for A_f, in that its order should be determined, up to a multiplicative constant, by those primes in $\mathcal{P}_L$. Pursuing this idea, let us define

$$N_{f,t}^{\mathrm{split}}(x) := \#\{p \in \mathcal{P}_L \mid p \leq x,\ b(p) = t\}.$$

Since the possible values of $a(p)$ such that $b(p) \equiv 0 \pmod p$ depend on the residue degree of the primes in F over p, it is clear that the distribution of the nonordinary values $b(p)$ in the interval

$$[-2^d p^{d/2},\, 2^d p^{d/2}]$$

cannot be uniform. Nevertheless, to get a rough idea of its order, let us assume initially that all the integers lying in $[-2^d p^{d/2}, 2^d p^{d/2}]$ had the same probability of being equal to $b(p)$. In this case,

$$N_{f,0}^{\mathrm{split}}(x) \sim \sum_{p \leq x} \frac{1}{2^{d+1} p^{d/2}},$$

$$\sum_{\substack{p \leq x \\ p \mid t}} N_{f,t}^{\mathrm{split}}(x) \sim \begin{cases} \sum_{p \leq x} 1/(4\sqrt{p}) & \text{if } d = 1, \\ \sum_{p \leq x} 1/p & \text{if } d > 1, \end{cases}$$

as $x \to \infty$ and for p running into $\mathcal{P}_L$. In particular, for $d > 2$, we would get only a finite number of primes for which $a(p) = 0$. Since $L/\mathbb{Q}$ is abelian, we have

$$\sum_{p \in \mathcal{P},\, p \leq x} \frac{1}{p^s} \sim \frac{1}{[L : \mathbb{Q}]} \sum_{p \leq x} \frac{1}{p^s} \quad \text{for } 0 < s \leq 1.$$

If $d > 1$, we get as a consequence that the number of nonordinary primes for A_f would be asymptotically equivalent to $\log \log x$, up to some multiplicative constant. If $d = 1$, then $F = \mathbb{Q}$ and $\dim B_f \leq 2$. In this case, we see that the asymptotic behaviour of the nonordinary primes would be that predicted by the results of [Lang and Trotter 1976], even if $\dim B_f = 2$. The next proposition shows that for $d = 1$, the condition $\dim B_f = 2$ implies $r(B_{f/\mathbb{F}_p}) \neq 1$, which explains why the values $r_p(A_f)$ behave in this case like those of the g-th power of an elliptic curve over $\mathbb{Q}$ (cf. Section 9).

Proposition 6.2. *If $F = \mathbb{Q}$, all the geometric fibres $\tilde{A}_{f,p}$, for $p \nmid N$, are isogenous to the gth-power of an elliptic curve.*

Proof. We know already that the claim is true if $a(p) = 0$. Assume instead that $a(p) \neq 0$ and let κ denote the residue degree of the primes in L over p. By Eichler–Shimura and 6.1, there exists an algebraic integer α_p such that

$$a(p) = \alpha_p + \bar{\alpha}_p \varepsilon(p), \quad \alpha_p \bar{\alpha}_p = p, \quad \alpha_p^\kappa + \bar{\alpha}_p^\kappa \in \mathcal{O}_F = \mathbb{Z}.$$

If A_f is nonordinary at p, then there is a prime $\mathfrak{p} \mid p$ in E such that $a(p) \equiv 0 \pmod{\mathfrak{p}}$. Hence, $\alpha_p^\kappa + \bar{\alpha}_p^\kappa \in p\mathbb{Z}$ and p divides $\alpha_p^{2\kappa}$, $\bar{\alpha}_p^{2\kappa}$, which implies that $r_p(A_f) = 0$ and $r(B_{f/\bar{\mathbb{F}}_p}) = 0$. Since $\dim B_f \leq 2$, the geometric fibre $B_{f/\bar{\mathbb{F}}_p}$ is isogenous to a power of a supersingular elliptic curve. Thus, the same is true for $\tilde{A}_{f,p}$.

Assume now that A_f is ordinary at p. Then $B_{f/\bar{\mathbb{F}}_p}$ is also ordinary. If $B_{f/\bar{\mathbb{F}}_p}$ were simple, then the algebra $\mathbb{Q} \otimes \mathrm{End}(B_{f/\bar{\mathbb{F}}_p})$ would be a number field, but this is impossible if $\dim B_f = 2$ since $\mathbb{Q} \otimes \mathrm{End}(B_{f/\bar{\mathbb{F}}_p})$ contains the noncommutative algebra $\mathbb{Q} \otimes \mathrm{End}(B_f)$. Since the characteristic polynomial of the relative Frobenius φ_{p^κ} acting on the Tate module of $A_{f/\mathbb{F}_{p^\kappa}}$ is a power of $x^2 - (\alpha_p^\kappa + \bar{\alpha}_p^\kappa)x + p^\kappa$, we see that the variety $\tilde{A}_{f,p}$ is isogenous to a power of an elliptic curve. $\square$

7. CHEBOTAREV DENSITIES IN GL_2-EXTENSIONS

For any number field K, we let $G_K := \mathrm{Gal}(\bar{\mathbb{Q}}/K)$. Let $A/\mathbb{Q}$ be any abelian variety of dimension g, l a prime, and

$$\rho_l : G_\mathbb{Q} \to \mathrm{Aut}(T_l(A)) \simeq \mathrm{GL}(2g, \mathbb{Z}_l)$$

the continuous l-adic representation defined by the Tate module. Let ρ be the homomorphism given by $\rho = \prod_l \rho_l$ where the product runs over the set of all prime numbers. We know [Serre 1985/86] that there exists a finite extension $K/\mathbb{Q}$ such that the subgroup $\rho(G_K)$ is open in the product $\prod_l \rho_l(G_K)$. If $A = A_f$, f as above, then ρ_l is equivalent to the l-adic representation of $G_\mathbb{Q}$ into $\mathrm{GL}(2, \mathcal{O}_E \otimes \mathbb{Z}_l)$ attached to f. In this case, we want to prove that $\rho(G_L)$ is open in $\prod_l \rho_l(G_L)$, where the field L is, as in Section 6, the abelian extension of $\mathbb{Q}$ cut out by the set of Dirichlet characters that intervene in the inner twists of f.

Lemma 7.1. *Let $\mathcal{O}$ be the integer ring of a number field. Let G be a closed subgroup of*

$$\prod_l \mathrm{GL}(2, \mathcal{O} \otimes \mathbb{Z}_l).$$

Denote by G_l the image of G under the projection in $\mathrm{GL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$. Suppose that

(a) *the image of G by $\det : \prod_l G_l \to \prod_l (\mathcal{O} \otimes \mathbb{Z}_l)^*$ is open in $\det(\prod_l G_l)$, and*
(b) *G_l contains $\mathrm{SL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$ for almost all l.*

Then G is open in $\prod_l G_l$.

Proof. The assertions for the case $\mathcal{O} = \mathbb{Z}$ correspond to the main lemma in [Serre 1989, Chapter 4]. We outline the required modifications in our case.

(i) The group $\mathrm{PSL}(2, \mathbb{F}_{l^\nu})$ is simple for any prime $l \geq 5$ and ν a positive integer. Every proper subgroup of this group is solvable or isomorphic to one of the following groups: $\mathrm{PSL}(2, \mathbb{F}_{l^m})$ for $m \mid \nu$, $\mathrm{PGL}(2, \mathbb{F}_{l^m})$ for $2m \mid \nu$, or the alternating group A_5. The last possibility occurs only if $l^{2\nu} \equiv 1 \pmod 5$ [Huppert 1967].

(ii) No proper subgroup of $\mathrm{SL}(2, \mathbb{F}_{l^\nu})$ can possibly map onto $\mathrm{PSL}(2, \mathbb{F}_{l^\nu})$, since the transvections generate $\mathrm{SL}(2, \mathbb{F}_{l^\nu})$ and have order l.

(iii) Let X be a closed subgroup of $\mathrm{SL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$ that maps onto $\mathrm{SL}(2, \mathcal{O}/l\mathcal{O})$. If $l \geq 5$, then $X = \mathrm{SL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$.

(iv) Let G be a closed subgroup of $\prod_l \mathrm{GL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$ (at this point, we do not require G to satisfy the conditions of 7.1). Let $X = \prod_l G_l$. Let S be a finite set of prime numbers, and $X_S = \prod_{l \in S} G_l$. The image G_S of G by the projection $X \to X_S$ is open in X_S.

(v) Assume now that a closed subgroup G of

$$\prod_l \mathrm{GL}(2, \mathcal{O} \otimes \mathbb{Z}_l)$$

satisfies (b). Let S be a finite set of prime numbers so that $\{2, 3, 5\}$ are in S and, if $l \notin S$, then

$\mathrm{GL}(2, \mathcal{O}\otimes\mathbb{Z}_l)$ contains $\mathrm{SL}(2, \mathcal{O}\otimes\mathbb{Z}_l)$. Then G contains $\prod_{l\notin S}\mathrm{SL}(2, \mathcal{O}\otimes\mathbb{Z}_l)$.

(vi) If G is as in (v), then G contains an open subgroup of $\prod_l \mathrm{SL}(2, \mathcal{O}\otimes\mathbb{Z}_l)\cap G_l$.

Suppose now that G satisfies (a) and (b). To finish the proof we take into account that the kernel of the homomorphism $\det : \prod_l G_l \to \prod_l(\mathcal{O}\otimes\mathbb{Z}_l)^*$ is $\prod_l \mathrm{SL}(2, \mathcal{O}\otimes\mathbb{Z}_l)\cap G_l$. Hence, by (vi), the kernel of $\det_{|G}$ is open in $\ker(\det)$. Since $\det(G)$ is an open subgroup of $\det(\prod_l G_l)$, we get that G is an open subgroup of $\prod_l G_l$. □

We turn now to the l-adic representations attached to the newform f. We denote by $\rho_{l,L}$ the restriction of ρ_l to G_L, and by ρ_L the restriction of ρ to G_L.

Lemma 7.2. *The image of $\rho_L(G_L)$ under the map $\det : \prod_l \rho_{l,L}(G_L) \to \prod_l \mathbb{Z}_l^*$ is open.*

Proof. Because $G_L \subseteq \ker(\varepsilon)$, the cyclotomic character is $\det(\rho_{L,l}) : G_L \to \mathbb{Z}_l^*$. The assertion follows as in [Serre 1989, Lemma IV, 3.1]. □

Since $\rho_l(G_L)$ contains $\mathrm{SL}(2, \mathcal{O}_F\otimes\mathbb{Z}_l)$ for almost all l, and from the above lemmas, the next proposition follows.

Proposition 7.3. *The subgroup $\rho(G_L)$ is open in the product $\prod_l \rho_l(G_L)$.*

We recall that F is the center of $\mathbb{Q}\otimes\mathrm{End}(B_f)$. Consider

$$\mathcal{O}_F\otimes\mathbb{Z}_l = \bigoplus_{\lambda|l}\mathcal{O}_\lambda,$$

where $\mathcal{O}_\lambda$ denotes the completion of the integer ring $\mathcal{O}_F$ at a prime ideal $\lambda\,|\,l$. By ρ_λ we denote the compositum of $\rho_{l,L}$ with the projection onto $\mathrm{GL}(2,\mathcal{O}_\lambda)$. Given an integral ideal $\mathfrak{m} = \prod \lambda^{n_\lambda}$ of $\mathcal{O}_F$, let

$$\rho_\mathfrak{m} = \prod_{\lambda|\mathfrak{m}} \rho_\lambda$$

and let $t_\mathfrak{m}$ denote the $(\mathrm{mod}\,\mathfrak{m})$-reduction homomorphism

$$\prod_{\lambda|\mathfrak{m}} \mathrm{GL}(2,\mathcal{O}_\lambda) \to \prod_{\lambda|\mathfrak{m}} \mathrm{GL}(2,\mathcal{O}_\lambda/\lambda^{n_\lambda}).$$

For a prime $\mathfrak{p}\,|\,p$ in L not dividing N, we note $\mathrm{Frob}_\mathfrak{p} = \mathrm{Frob}_\mathfrak{p}(M/L)$, where M is now the field cut out by ρ_L. We denote, for simplicity,

$$a(\mathfrak{p}) = \alpha_p^\kappa + \bar\alpha_p^\kappa,$$

where κ is the residue degree of $\mathfrak{p}$, $a(p) = \alpha_p + \bar\alpha_p\varepsilon(p)$, and $\alpha_p\bar\alpha_p = p$. Observe that

$$a(\mathfrak{p}) = \mathrm{Tr}(\rho_{l,L}(\mathrm{Frob}_\mathfrak{p})) \quad \text{for all } l \neq p.$$

For each nonzero integral ideal $\mathfrak{m}$ of $\mathcal{O}_F$, and for any element $\theta\in\mathcal{O}_F$, we define $\pi_\mathfrak{m}(\theta)$ as

$$N_{F/\mathbb{Q}}(\mathfrak{m}) \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid N_{L/\mathbb{Q}}(\mathfrak{p}) \le x,\ a(\mathfrak{p}) \equiv \theta \,(\mathrm{mod}\,\mathfrak{m})\}}{\#\{\mathfrak{p} \mid N_{L/\mathbb{Q}}(\mathfrak{p}) \le x\}},$$

where $\mathfrak{p}$ runs into the set of primes in L that do not divide N. The Chebotarev density theorem guarantees the existence of the limit. Observe that

$$\sum_{\theta\in\mathcal{O}_F/\mathfrak{m}} \frac{\pi_\mathfrak{m}(\theta)}{N_{F/\mathbb{Q}}(\mathfrak{m})} = 1,$$

which tells us that the average value of $\pi_\mathfrak{m}$ is 1.

Proposition 7.3 will be used to establish the uniform convergence of the sequence $\{\pi_\mathfrak{m}\}$ when the indices $\mathfrak{m}$ run into the filter of all nonzero ideals of the ring $\mathcal{O}_F$. Before that we need the following lemma:

Lemma 7.4. *Let l be a prime number and let m, ν denote positive integers such that m divides ν. Put $G := \mathrm{GL}(2,\mathbb{F}_{l^\nu})$, $G_m := \{s\in G \mid \det(s)\in\mathbb{F}_{l^m}\}$, and $G_{m,e} := \{s\in G_m \mid \mathrm{Tr}(s) = e\}$ for $e\in\mathbb{F}_{l^\nu}$. Then:*

(i) $\#G = l^\nu(l^\nu-1)^2(l^\nu+1)$ *and* $\#G_m = l^\nu(l^\nu-1)\times(l^\nu+1)(l^m-1)$.

(ii) $\#G_{m,0} = \begin{cases} l^{2\nu}(l^m-1) & \text{if } 2m\nmid\nu, \\ l^\nu(l^\nu+1)(l^m-1) & \text{if } 2m\mid\nu. \end{cases}$

(iii) $l^\nu(l^\nu-1)(l^m-1) \le \#G_{m,e} \le l^\nu(l^\nu+1)(l^m-1)$ *for all* $e\in\mathbb{F}_{l^\nu}$.

(iv) $\#G_{\nu,e} = l^\nu(l^{2\nu}-l^\nu-1)$ *for all* $e\neq 0$.

Theorem 7.5. (i) *There exists a bounded function $\pi : \mathcal{O}_F\to\mathbb{R}$ such that $\lim_\mathfrak{m}\pi_\mathfrak{m} = \pi$ and the convergence is uniform.*

(ii) *There exist both an ideal* $\mathfrak{n} \neq (0)$ *of* $\mathcal{O}_F$ *and constants* $0 < \tilde{c}_1 < \tilde{c}_2$ *such that for all* $\theta \in \mathcal{O}_F$ *is* $\tilde{c}_1 \pi_{\mathfrak{n}}(\theta) \leq \pi(\theta) \leq \tilde{c}_2 \pi_{\mathfrak{n}}(\theta)$.

Proof. Since, by 7.3, $\rho(G_L)$ is an open subgroup of $\prod_l (\prod_{\lambda | l} \rho_\lambda(G_L))$, there is a nonzero ideal $\mathfrak{n}$ of $\mathcal{O}_F$ satisfying the following properties:

- if $\lambda \nmid \mathfrak{n}$, then
$$\rho_\lambda(G_L) = \{s \in \mathrm{GL}(2, \mathcal{O}_\lambda) \mid \det s \in \mathbb{Z}_l^*\}.$$
- $\rho(G_L) = \prod_{\lambda \nmid \mathfrak{n}} \rho_\lambda(G_L) \times \rho_{\mathfrak{n}}(G_L)$.
- $t_{\mathfrak{n}}^{-1}(t_{\mathfrak{n}} \rho_{\mathfrak{n}}(G_L)) = \rho_{\mathfrak{n}}(G_L)$.

Let ν denote the residue degree of a prime ideal λ over l and $\lambda \nmid \mathfrak{n}$. By the preceding lemma, we get $l^\nu/(l^\nu + 1) \leq \pi_\lambda(\theta) \leq l^\nu/(l^\nu - 1)$. If $\nu = 1$ we get, moreover,

$$\pi_\lambda(\theta) = \begin{cases} l^2/(l^2 - 1) & \text{if } \theta \equiv 0 \pmod{\lambda}, \\ (l^3 - l^2 - l)/(l^3 - l^2 - l + 1) & \\ & \text{if } \theta \not\equiv 0 \pmod{\lambda}. \end{cases}$$

Hence, the infinite product $\prod_{\lambda \nmid \mathfrak{n}} \pi_\lambda(\theta)$ is absolutely convergent. Let $c(\theta) := \prod_{\lambda \nmid \mathfrak{n}} \pi_\lambda(\theta)$. If $\mathfrak{n} \mid \mathfrak{m}$, then

$$\pi_{\mathfrak{m}}(\theta) = \pi_{\mathfrak{n}}(\theta) \prod_{\lambda | \mathfrak{m}, \lambda \nmid \mathfrak{n}} \pi_\lambda(\theta).$$

Thus, $\lim_{\mathfrak{m}} \pi_{\mathfrak{m}}(\theta) = \pi_{\mathfrak{n}}(\theta) c(\theta)$. We denote this limit by $\pi(\theta)$. We consider the constants

$$c_{1,\lambda} := \begin{cases} 1/(1 + l^{-\nu}) & \text{if } \nu > 1, \\ 1 & \text{if } \nu = 1, \end{cases}$$
$$c_{2,\lambda} := \begin{cases} 1/(1 - l^{-\nu}) & \text{if } \nu > 1 \\ 1/(1 - l^{-2}) & \text{if } \nu = 1, \end{cases}$$
$$\tilde{c}_1 := \prod_{\lambda \nmid \mathfrak{n}} c_{1,\lambda},$$
$$\tilde{c}_2 := \prod_{\lambda \nmid \mathfrak{n}} c_{2,\lambda}.$$

For each $\theta \in \mathcal{O}_F$ we have $c_{1,\lambda} \leq \pi_\lambda(\theta) \leq c_{2,\lambda}$ and $\tilde{c}_1 \leq c(\theta) \leq \tilde{c}_2$. Note that if $\mathfrak{m} \geq \mathfrak{n}$, then $\pi_{\mathfrak{m}}(\theta) \leq c$ for $c := N_{F/\mathbb{Q}}(\mathfrak{n}) \tilde{c}_2$. The convergence of the sequence is uniform since, for all $\mathfrak{m} \geq \mathfrak{n}$, we have

$$|\pi(\theta) - \pi_{\mathfrak{m}}(\theta)| = \pi_{\mathfrak{m}}(\theta) \left| \prod_{\lambda \nmid \mathfrak{m}} \pi_\lambda(\theta) - 1 \right| \leq c \left| \prod_{\lambda \nmid \mathfrak{m}} c_{2,\lambda} - 1 \right|$$

and

$$\lim_{\mathfrak{m}} \prod_{\lambda \nmid \mathfrak{m}} c_{2,\lambda} = 1. \qquad \square$$

8. A PROBABILISTIC MODEL AND CONJECTURES

To predict more precisely the number of nonordinary primes for A_f, and of those for which $r_p(A_f)$ vanishes, which we can find up to a given value, we construct a probabilistic model. It generalizes the one introduced in [Lang and Trotter 1976] for the elliptic curves defined over $\mathbb{Q}$. We keep the notations of Section 7.

Let Σ be the set of all prime ideals of the integer ring of L. Because

$$\lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in \Sigma \mid N_{L/\mathbb{Q}}(\mathfrak{p}) = p \leq x\}}{\#\{\mathfrak{p} \in \Sigma \mid N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x\}} = 1,$$

we can rewrite $\pi_{\mathfrak{m}}(\theta)$ as

$$N_{F/\mathbb{Q}}(\mathfrak{m}) \lim_{x \to \infty} \frac{\#\{p \in \mathcal{P}_L \mid p \leq x,\ a(p) \equiv \theta \pmod{\mathfrak{m}}\}}{\#\{p \in \mathcal{P}_L \mid p \leq x\}},$$

and see that the functions $\pi_{\mathfrak{m}}$ are determined by the primes in $\mathcal{P}_L$.

Let $\{\tau_1, \dots, \tau_d\}$ be the set of all $\mathbb{Q}$-embeddings of F into $\bar{\mathbb{Q}}$. Let $\tau : F \to \mathbb{R}^d$ denote the geometric representation of F, given by $\tau(\alpha) = (\alpha^{(1)}, \dots, \alpha^{(d)})$ for α in F and $\alpha^{(i)} := \alpha^{\tau_i}$. We note that if $p \in \mathcal{P}_L$, then $a(p)^{(i)}$ is defined and $|a(p)^{(i)}| \leq 2p^{1/2}$ with $1 \leq i \leq d$.

We now list and comment on our assumptions concerning the probabilistic model.

H1. There exists a positive continuous function $\pi_\infty : \mathbb{R}^d \to \mathbb{R}$ with support in $[-1, 1]^d$ such that, for any Lebesgue measurable subset $X \subseteq \mathbb{R}^d$,

$$\int_X \pi_\infty = \lim_{x \to \infty} \frac{\#\left\{p \in \mathcal{P}_L \mid p \leq x,\ \dfrac{\tau(a(p))}{2\sqrt{p}} \in X\right\}}{\#\{p \in \mathcal{P}_L \mid p \leq x\}}.$$

In the case of elliptic curves defined over $\mathbb{Q}$, it is conjectured that the measure attached to the density function π_∞ corresponds to the Sato–Tate measure $(2/\pi)\sin^2\alpha d\alpha$, once the set of conjugacy classes of $\mathrm{SU}(2)$ is identified with $[-1,1]$ (compare [Lang and Trotter 1976; Tate 1965]). For an insight in the general case, consider the Mumford–Tate group $G_M(B_f)$ and the kernel G^1 of the canonical homomorphism of $G_M(B_f)$ in the multiplicative group $\mathbb{G}_m$. Let K be the maximal compact subgroup of $G^1(\mathbb{C})$ and $\mathrm{Cl}\,K$ the set of its conjugacy classes. Put in $\mathrm{Cl}\,K$ the image of the Haar measure of K. It seems reasonable to suspect that this measure should provide the measure attached to π_∞.

H2. For each $p \in \mathcal{P}_L$ and for each nonzero ideal $\mathfrak{m}$ in $\mathcal{O}_F$, there exists a constant $c(p,\mathfrak{m}) > 0$ such that the function $g_\mathfrak{m} : \mathcal{P}_L \times \mathcal{O}_F \to \mathbb{R}$ defined by

$$g_\mathfrak{m}(p,\theta) = c(p,\mathfrak{m})\,\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\,\pi_\mathfrak{m}(\theta)$$

satisfies $\sum_{\theta\in\mathcal{O}_F} g_\mathfrak{m}(p,\theta)=1$ for almost all $p\in\mathcal{P}_L$.

H3. For each $p \in \mathcal{P}_L$, there exists a constant $c_p > 0$ such that the function $g : \mathcal{P}_L \times \mathcal{O}_F \to \mathbb{R}$ defined by

$$g(p,\theta) = c_p\,\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\,\pi(\theta)$$

satisfies $\sum_{\theta\in\mathcal{O}_F} g(p,\theta) = 1$ for almost all $p \in \mathcal{P}_L$.

If $a(p') = 0$ for some $p' \in \mathcal{P}_L$, then $\pi_\mathfrak{m}(0) > 0$ for all $\mathfrak{m}$. Thus $\pi(0) > 0$. If, moreover, $\pi_\infty(0) > 0$, then H2 and H3 follow from H1.

The next result yields the asymptotic behaviour of the family of constants introduced in H2, H3.

Theorem 8.1. *Assume* H1 *and* H2, *and let d, D denote the degree and the discriminant, respectively, of $F/\mathbb{Q}$.*

(i) *For each nonzero ideal $\mathfrak{m}$ of $\mathcal{O}_F$, we have*

$$c(p,\mathfrak{m}) \sim \frac{\sqrt{|D|}}{2^d p^{d/2}} \qquad \text{as } p\to\infty.$$

(ii) *Assume, moreover, that* H3 *holds. Then $c_p = \lim_\mathfrak{m} c(p,\mathfrak{m})$ and*

$$c_p \sim \frac{\sqrt{|D|}}{2^d p^{d/2}} \qquad \text{as } p\to\infty.$$

Proof. Let $\{e_i\}$ be the canonical basis of $\mathbb{R}^d$. Fix $\mathfrak{m}$ and choose a basis $\{u_i\}$ of the lattice $\tau(\mathfrak{m})$. Let U be the linear automorphism of $\mathbb{R}^d$ defined by $U(e_i) = u_i$ for $1 \le i \le d$. Since

$$|\det U| = \sqrt{|D|}\,N_{F/\mathbb{Q}}(\mathfrak{m}),$$

we have

$$1 = \int_{\mathbb{R}^d}\pi_\infty = \sqrt{|D|}\,N_{F/\mathbb{Q}}(\mathfrak{m})\int_{\mathbb{R}^d}\pi_\infty\circ U.$$

We approximate the integral by Riemann sums:

$$\int_{\mathbb{R}^d}\pi_\infty\circ U = \lim_{p\to\infty}\frac{1}{2^d p^{d/2}}\sum_{(t_n)\in\mathbb{Z}^d}\pi_\infty\Big(U\Big(\frac{t_1}{2\sqrt{p}},\dots,\frac{t_d}{2\sqrt{p}}\Big)\Big).$$

Let $\theta_0 \in \mathcal{O}_F$. Since π_∞ and U are uniformly continuous, we get

$$\lim_{p\to\infty}\int_{\mathbb{R}^d}\pi_\infty\circ\Big(\frac{\tau(\theta_0)}{\sqrt{2p}}+U\Big) = \lim_{p\to\infty}\frac{1}{2^d p^{d/2}}\sum_{(t_n)\in\mathbb{Z}^d}\pi_\infty\Big(\frac{\tau(\theta_0)}{\sqrt{2p}}+U\Big(\frac{t_1}{2\sqrt{p}},\dots,\frac{t_d}{2\sqrt{p}}\Big)\Big).$$

Thus,

$$\int_{\mathbb{R}^d}\pi_\infty\circ U = \lim_{p\to\infty}\int_{\mathbb{R}^d}\pi_\infty\circ\Big(\frac{\tau(\theta_0)}{\sqrt{2p}}+U\Big) = \lim_{p\to\infty}\frac{1}{2^d p^{d/2}}\sum_{\theta\in\theta_0+\mathfrak{m}}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big).$$

By multiplying the last equality by $\pi_\mathfrak{m}(\theta_0)$ and summing over the congruence classes θ_0 in $\mathcal{O}_F/\mathfrak{m}$, we get

$$\lim_{p\to\infty}\frac{\sqrt{|D|}}{2^d p^{d/2}}\sum_{\theta\in\mathcal{O}_F}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\pi_\mathfrak{m}(\theta) = 1.$$

We easily see that H2 implies (i).

From H2 and H3, it is clear that $\lim_{\mathfrak{m}} c(p,\mathfrak{m}) = c_p$. By using (i), we get for all $\mathfrak{m}$

$$\lim_{p\to\infty}\left|\frac{\sqrt{|D|}}{2^d p^{d/2}}\sum_{\theta\in\mathcal{O}_F}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\pi(\theta)-1\right| \le \lim_{p\to\infty}\frac{\sqrt{|D|}}{2^d p^{d/2}}\sum_{\theta\in\mathcal{O}_F}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\,|\pi(\theta)-\pi_{\mathfrak{m}}(\theta)|.$$

By thorem 7.5 and applying (i) for $\mathfrak{m} = (1)$, we get

$$\lim_{p\to\infty}\frac{\sqrt{|D|}}{2^d p^{d/2}}\sum_{\theta\in\mathcal{O}_F}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p}}\Big)\pi(\theta) = 1.$$

Now (ii) follows from H3. □

Remark. From theorem 8.1, it follows that

$$\lim_{\mathfrak{m}} g_{\mathfrak{m}}(p,\theta) = g(p,\theta)$$

for almost all $p\in\mathcal{P}_L$. The functions $g_{\mathfrak{m}}(p,-)$ and $g(p,-)$ can be interpreted as probability distributions of random variables $Y_{p,\mathfrak{m}}$ and Y_p, respectively, with target in the adeles of F, so that $\lim_{\mathfrak{m}}\operatorname{Prob}\{Y_{p,\mathfrak{m}}=\tau(\theta)\} = \operatorname{Prob}\{Y_p=\tau(\theta)\}$. That is, the sequence of random variables $\{Y_{p,\mathfrak{m}}\}$ converges in law to Y_p.

Given a real number $x\ge 2$, we define

$$P^{\text{split}}_{f,\theta}(x) = \#\{p\in\mathcal{P}_L \mid p\le x,\ a(p)=\theta\}.$$

We may assume that the asymptotic distribution of the values $a(p)$, for $p\in\mathcal{P}_L$, is given by the random variable Y_p. Then, up to an additive constant, $P^{\text{split}}_{f,\theta}(x)$ is asymptotically equivalent to

$$\sum_{p\in\mathcal{P},p\le x} g(p,\theta)$$

as $x\to\infty$. For $\theta=0$, we get

$$\sum_{p\in\mathcal{P},p\le x} g(p,0)\sim\frac{\sqrt{|\,D\,|}}{2^d}\pi_\infty(0)\pi(0)\sum_{p\in\mathcal{P},p\le x}\frac{1}{p^{d/2}}$$

as $x\to\infty$.

Let $\mathfrak{n}$ be the ideal of $\mathcal{O}_F$ as in 7.5. The density of primes p such that $a(p)\in\mathfrak{n}\mathcal{O}_E$ is greater than zero, since we are considering l-adic representations that are odd. Thus, it should be $\pi_{\mathfrak{n}}(0)>0$, in which case $\pi(0)>0$. Since Sato–Tate density attains its maximum at 0, it should be $\pi_\infty(0)\pi(0)>0$.

Putting all this together, we generalize the Lang and Trotter conjecture on the distribution law of supersingular primes in the elliptic case in the following conjecture:

Conjecture 8.2. *Let $f\in S_2(N,\varepsilon)$ be a newform without complex multiplication. Let $d=[F:\mathbb{Q}]$. Let $P_{A_f,0}(x)$ denote the number the primes $p\le x$ for which $r_p(A_f)=0$. There exist constants $C_{f,0}>0, C_f$ such that*

$$P_{A_f,0}(x)\sim C_{f,0}\sum_{p\le x}\frac{1}{p^{d/2}}+C_f\quad \text{as } x\to\infty.$$

Remark. Conjecture 1 amounts to saying that there should exist constants $c_{f,0}>0$ such that

$$P_{A_f,0}(x)\begin{cases}\sim c_{f,0}\sqrt{x}/\log x & \text{if } d=1,\\ \sim c_{f,0}\log\log x & \text{if } d=2,\\ =O(1) & \text{if } d>2.\end{cases}$$

We should emphasize that the function $P_{f,0}$ should exhibit the same asymptotical behaviour since

$$P_{f,0}(x) = P_{A_f,0}(x)+O(1);$$

compare 5.2(i).

Next we deal with the nonordinary reductions of A_f, which are more difficult to handle.

Lemma 8.3. *Let $\{\mathfrak{p}_m\}$ be a sequence of prime ideals of $\mathcal{O}_F$, with constant residue degree ν, such that the sequence of their norms $\{p_m\}$ tends monotonically to infinity. Assume that $p_m\in\mathcal{P}_L$ for all m, as well as* H1, H2. *For each nonzero ideal $\mathfrak{m}$ of $\mathcal{O}_F$, we have*

$$\sum_{\theta\in\mathfrak{p}_m} g_{\mathfrak{m}}(p_m,\theta)\begin{cases}\sim \pi_\infty(0)\pi_{\mathfrak{m}}(0)\sqrt{|D|}/(2^d p_m^{d/2}) & \text{if } \nu>d/2,\\ =O(p_m^{-d/2}) & \text{if } \nu=d/2,\\ \sim 1/p_m^{\nu} & \text{if } \nu<d/2,\end{cases}$$

as $p_m\to\infty$.

Proof. *Case $\nu>d/2$.* For any $\theta\in\mathfrak{p}_m$ such that $\tau(\theta)\in[-2\sqrt{p}_m,\,2\sqrt{p}_m]^d$, we have $N_{F/\mathbb{Q}}(\theta)=kp_m^{\nu}$, where $k\in\mathbb{Z}$ and $|k|\le 2^d p_m^{d/2-\nu}$. If p_m is large enough, the inequality implies $k = 0$ and $\theta = 0$. Thus,

$$\sum_{\theta\in\mathfrak{p}_m} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big)\pi_{\mathfrak{m}}(\theta) = \pi_\infty(0)\pi_{\mathfrak{m}}(0).$$

By 8.1(i), the assertion follows.

Case $\nu = d/2$. Let $0 \neq \theta \in \mathfrak{p}_m$ be chosen so that $\tau(\theta) \in [-2\sqrt{p_m},\, 2\sqrt{p_m}]^d$. There exists an ideal $\mathfrak{a}$ of $\mathcal{O}_F$ such that $(\theta) = \mathfrak{p}_m\mathfrak{a}$ with $1 \leq N_{F/\mathbb{Q}}(\mathfrak{a}) \leq 2^d$. Denoting by s_1 the number of ideals $\mathfrak{a}$ for which $N_{F/\mathbb{Q}}(\mathfrak{a}) \leq 2^d$, we see that there are at most s_1 principal ideals (θ) that satisfy $\theta \in \mathfrak{p}_m$ and $\tau(\theta) \in [-2\sqrt{p}_m,\, 2\sqrt{p}_m]^d$. We fix (θ). From all generators of (θ) as a principal ideal, we only consider those whose image under τ lies in $[-2\sqrt{p_m},\, 2\sqrt{p_m}]^d$. We shall prove that their number is bounded by a constant that does not depend on p_m. Indeed, consider

$$|\theta^{(i)}| = \frac{|N_{F/\mathbb{Q}}(\theta^{(i)})|}{\prod_{j\neq i}|\theta^{(j)}|} \geq \frac{N_{F/\mathbb{Q}}(\mathfrak{a})p_m^{d/2}}{2^{d-1}p_m^{(d-1)/2}} \geq \frac{p_m^{1/2}}{2^{d-1}}.$$

Let ξ a unit of $\mathcal{O}_F$. The conditions $|\xi^{(i)}\theta^{(i)}| \leq 2p_m^{1/2}$, for $1 \leq i \leq d$, force $|\xi^{(i)}| \leq 2^d$ for all i. The set of units that satisfy these inequalities is finite. Let s_2 denote its number and M an upper bound for the function π_∞. By taking into account $\theta = 0$, and if $s := s_1 s_2 + 1$, we get

$$\sum_{\theta\in\mathfrak{p}_m} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big) \leq Ms,$$
$$\sum_{\theta\in\mathfrak{p}_m} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big)\pi_{\mathfrak{m}}(\theta) \leq MsN_{F/\mathbb{Q}}(\mathfrak{m}),$$

since $\pi_{\mathfrak{m}}(\theta) \leq N_{F/\mathbb{Q}}(\mathfrak{m})$. By 8.1(i), the assertion follows.

Case $\nu < d/2$. Now $d/2-\nu \geq 1/2$ and, in particular, $1/2-\nu/d \geq 1/(2d)$. We denote by $\{e_1,\dots,e_d\}$ a basis of the lattice $\tau(\mathcal{O}_F)$. For $x = (x_i)$, $y = (y_i) \in \mathbb{R}^d$, we define $xy := (x_i y_i)$, so that we have the rule $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta)$. Let $\{\xi_1,\dots,\xi_{d-1}\}$ be a system of fundamental units of $\mathcal{O}_F$.

We first show that for any integer $m > 0$ there is a basis $\{u_{1,m},\dots,u_{d,m}\}$ of the lattice $\tau(\mathfrak{m}\mathfrak{p}_m)$ such that

$$0 < k_1 p_m^{\nu/d} \leq |u_{n,m}^{(j)}| \leq k_2 p_m^{\nu/d} \quad \text{for } 1 \leq n, j \leq d.$$

Here k_1, k_2 are constants independent of m, and $u_{n,m}^{(j)} := (\tau^{-1}(u_{n,m}))^{(j)}$. Assume first that $\mathfrak{m}\mathfrak{p}_m$ is a principal ideal. We may choose a generator α_m in $\mathfrak{m}\mathfrak{p}_m$ such that

$$\log(|\alpha_m^{(j)}|) = \log(N_{F/\mathbb{Q}}(\mathfrak{m})^{1/d}p_m^{\nu/d}) + \sum_{k=1}^{d-1}\delta_k\log(|\xi_k^{(j)}|)$$

where $0 \leq \delta_k \leq 1$, and $1 \leq j \leq n$ [Hecke 1981]. Let $c_1, c_2 > 0$ be real numbers that only depend on $\{\xi_k^{(j)}\}$ and satisfy

$$c_1 N_{F/\mathbb{Q}}(\mathfrak{m})^{1/d}p_m^{\nu/d} \leq |\alpha_m^{(j)}| \leq c_2 N_{F/\mathbb{Q}}(\mathfrak{m})^{1/d}p_m^{\nu/d}$$

for $1 \leq j \leq d$. It suffices to define $u_{n,m} := \tau(\alpha_m)e_n$ for $1 \leq n \leq d$, and adjust the bounding constants k_1, k_2, accordingly. Fix now an ideal class of $\mathcal{O}_F$ and consider all ideals $\mathfrak{m}\mathfrak{p}_m$ that belong to it. Take an integral ideal $\mathfrak{a}$ such that all ideals $\mathfrak{a}\mathfrak{m}\mathfrak{p}_m$ are principal. By applying the preceding result to them, we get bases of the lattices $\tau(\mathfrak{a}\mathfrak{m}\mathfrak{p}_m)$ with bounding constants $N_{F/\mathbb{Q}}(\mathfrak{a})^{1/d}k_1$ and $N_{F/\mathbb{Q}}(\mathfrak{a})^{1/d}k_2$. Here k_1 and k_2 are the constants obtained before. Let $t \in \mathrm{GL}(n,\mathbb{R})$ be such that $t(\tau(\mathcal{O}_F)) = \tau(\mathfrak{a})$. Clearly, $t(\tau(\mathfrak{m}\mathfrak{p}_m)) = \tau(\mathfrak{a}\mathfrak{m}\mathfrak{p}_m)$. We choose the basis of $\tau(\mathfrak{m}\mathfrak{p}_m)$ by applying t^{-1} to the chosen basis in the principal case. By taking into account the finiteness of the class number, the existence of the basis $\{u_{n,m}\}$ follows in all the cases.

Choose now a system of representatives $\{\theta_i\}$, $1 \leq i \leq s$, of $\mathcal{O}_F/\mathfrak{m}$. Without loss of generality, we may assume that $\mathfrak{p}_m \nmid \mathfrak{m}$, since this is obviously true for $p_m > N_{F/\mathbb{Q}}(\mathfrak{m})$. Thus,

$$\sum_{\theta\in\mathfrak{p}_m} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big)\pi_{\mathfrak{m}}(\theta) = \sum_{i=1}^{s}\pi_{\mathfrak{m}}(\theta_i)\sum_{\substack{\theta\in\mathfrak{p}_m\\ \theta\in\theta_i+\mathfrak{m}}}\pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big).$$

Let $\theta_{i,m}$ be chosen so that $\theta_{i,m} \equiv 0 \pmod{\mathfrak{p}_m}$ and $\theta_{i,m} \equiv \theta_i \pmod{\mathfrak{m}}$. It suffices to prove that

$$\frac{\sqrt{|D|}}{2^d p_m^{d/2-\nu}} \sum_{\theta \in \theta_{i,m}+\mathfrak{p}_m\mathfrak{m}} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big) \sim \frac{1}{N_{F/\mathbb{Q}}(\mathfrak{m})}$$

as $p_m \to \infty$. Afterwards, multiplying by $\pi_{\mathfrak{m}}(\theta_{i,m})$ and by 8.1(i), the result will follow. Consider the affine automorphism

$$U_{i,m}(x_1,\dots,x_d) := \frac{\tau(\theta_{i,m})}{2\sqrt{p_m}} + \sum_{n=1}^d x_n u_{n,m}$$

and put $V_{i,m} = U_{i,m}^{-1}([-1,1]^d)$. Clearly,

$$1 = \int_{\mathbb{R}^d} \pi_\infty = \sqrt{|D|} N_{F/\mathbb{Q}}(\mathfrak{m}) p_m^\nu \int_{\mathbb{R}^d} \pi_\infty \circ U_{i,m},$$
$$\int_{V_{i,m}} 1 = \frac{2^d}{\sqrt{|D|} N_{F/\mathbb{Q}}(\mathfrak{m}) p_m^\nu}.$$

Note $v_{i,m}$ this last expression. For $(t_n) \in \mathbb{Z}^d$, we consider the cubes

$$\prod_{n=1}^d \Big[\frac{t_n}{2\sqrt{p_m}}, \frac{t_n+1}{2\sqrt{p_m}}\Big],$$

which satisfy

$$U_{i,m}\Big(\prod_{n=1}^d \Big[\frac{t_n}{2\sqrt{p_m}}, \frac{t_n+1}{2\sqrt{p_m}}\Big]\Big) \cap [-1,1]^d \neq \varnothing,$$

and denote their union by $H_{i,m}$. Consider now only those cubes that have a nonempty intersection with the boundary of $H_{i,m}$. Since $0 \le k_1 p_m^{\nu/d} \le |u_{n,m}^{(j)}|$ for $1 \le n, j \le d$, their number is $O(p_m^{(d-1)(1/2-\nu/d)})$. The volume of their union is $O(p_m^{(d-1)(1/2-\nu/d)-d/2})$. Since $(d-1)(1/2-\nu/d) - d/2 \le -1/(2d) - \nu$, we get

$$\int_{H_{i,m}} 1 = v_{i,m} + O(p_m^{-1/(2d)-\nu})$$
$$= p_m^{-\nu}\Big(\frac{2^d}{\sqrt{|D|} N_{F/\mathbb{Q}}(\mathfrak{m})} + O(p_m^{-1/(2d)})\Big).$$

By H1, for each $\varepsilon > 0$ there exists a $\delta > 0$ such that if $x, y \in \prod_{n=1}^d [a_n, b_n]$, with $|b_n - a_n| < \delta$ for all n, then $|\pi_\infty(x) - \pi_\infty(y)| < \varepsilon$. Now, by considering those primes p_m such that $dk_2 p_m^{\nu/d-1/2} < \delta$, and setting $W_{i,m} = \pi_\infty \circ U_{i,m}$, we get

$$\Big|\int_{\mathbb{R}^d} W_{i,m} - \frac{1}{2^d p_m^{d/2}} \sum_{(t_n)\in\mathbb{Z}^d} W_{i,m}\Big(\frac{t_1}{2\sqrt{p_m}}, \dots, \frac{t_d}{2\sqrt{p_m}}\Big)\Big| < \varepsilon \int_{H_{i,m}} 1.$$

Since

$$\sum_{(t_n)\in\mathbb{Z}^d} W_{i,m}\Big(\frac{t_1}{2\sqrt{p_m}}, \dots, \frac{t_d}{2\sqrt{p_m}}\Big) = \sum_{\theta-\theta_{i,m}\in\mathfrak{p}_m} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big),$$

we get

$$\Big|\sum_{\theta\in\theta_{i,m}+\mathfrak{m}\mathfrak{p}_m} \frac{1}{2^d p_m^{d/2-\nu}} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big) - \frac{1}{N_{F/\mathbb{Q}}(\mathfrak{m})\sqrt{|D|}}\Big| < \frac{\varepsilon 2^d}{\sqrt{|D|} N_{F/\mathbb{Q}}(\mathfrak{m})} + O(p_m^{-1/2d}).$$

Therefore,

$$\lim_{m\to\infty} \sum_{\theta\in\theta_{i,m}+\mathfrak{m}\mathfrak{p}_m} \frac{1}{2^d p_m^{d/2-\nu}} \pi_\infty\Big(\frac{\tau(\theta)}{2\sqrt{p_m}}\Big) = \frac{1}{N_{F/\mathbb{Q}}(\mathfrak{m})\sqrt{|D|}},$$

which concludes the proof. □

We denote by $\mathcal{P}_{LF}$ the set of primes $p \nmid N$ that split completely in LF.

Theorem 8.4. *Assume* H1 *and* H2, *and let* $d = [F:\mathbb{Q}]$.

(i) *Let* $\mathfrak{m}$ *be a nonzero ideal of* $\mathcal{O}_F$. *If* $d \ge 2$ *then* $\sum_{\{\theta: p | N_{F/\mathbb{Q}}(\theta)\}} g_{\mathfrak{m}}(p,\theta) = O(p^{-1})$ *as* $p \to \infty$, $p \in \mathcal{P}_L$. *If* $d > 2$ *we have*

$$\frac{1}{p} \le \sum_{\{\theta: p | N_{F/\mathbb{Q}}(\theta)\}} g_{\mathfrak{m}}(p,\theta) \le \frac{d}{p}$$

as $p \to \infty$, $p \in \mathcal{P}_{LF}$.

(ii) *Furthermore, assume* H3. *If* $d \ge 2$ *then*

$$\sum_{\{\theta: p | N_{F/\mathbb{Q}}(\theta)\}} g(p,\theta) = O(p^{-1})$$

as $p \to \infty$, $p \in \mathcal{P}_L$. *If* $d > 2$ *then*

$$\frac{\tilde{c}_1}{p} \le \sum_{\{\theta : p \mid N_{F/\mathbb{Q}}(\theta)\}} g(p,\theta) \le \frac{\tilde{c}_2 d}{p}$$

as $p \to \infty$, $p \in \mathcal{P}_{LF}$, *where* $0 < \tilde{c}_1 < \tilde{c}_2$ *are the constants introduced in theorem* 7.5.

Proof. Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{i_p}\}$ be the different prime ideals of $\mathcal{O}_F$ over $p \in \mathcal{P}_L$. We have

$$\sum_{\{\theta : p \mid N_{F/\mathbb{Q}}(\theta)\}} g_{\mathfrak{m}}(p,\theta) \le \sum_{\theta \in \mathfrak{p}_1} g_{\mathfrak{m}}(p,\theta) + \dots + \sum_{\theta \in \mathfrak{p}_{i_p}} g_{\mathfrak{m}}(p,\theta).$$

For each prime $p \in \mathcal{P}_L$, let $\mathfrak{p}_p \mid p$ denote a prime ideal for which the sum $\sum_{\theta \in \mathfrak{p}_p} g_{\mathfrak{m}}(p,\theta)$ attains its maximum value. Then

$$\sum_{\theta \in \mathfrak{p}_p} g_{\mathfrak{m}}(p,\theta) \le \sum_{\{\theta : p \mid N_{F/\mathbb{Q}}(\theta)\}} g_{\mathfrak{m}}(p,\theta) \le d \sum_{\theta \in \mathfrak{p}_p} g_{\mathfrak{m}}(p,\theta).$$

To get (i), it suffices to apply 8.3.

Let $\mathfrak{n}$ be an ideal as in 7.5. We have

$$\tilde{c}_1 \sum_{\theta} g_{\mathfrak{n}}(p,\theta) \le \sum_{\theta} g(p,\theta) \le \tilde{c}_2 \sum_{\theta} g_{\mathfrak{n}}(p,\theta)$$

as $p \to \infty$, $p \in \mathcal{P}_L$. Here the sum runs over the elements θ such that $p \mid N_{F/\mathbb{Q}}(\theta)$. To get (ii), it suffices now to apply (i). □

At this point, as a higher-dimensional analogue of the Lang and Trotter conjecture, it seems natural to state the following conjecture:

Conjecture 8.5. *We let* $f \in S_2(N,\varepsilon)$ *be a newform without complex multiplication. Assume that* $d \ge 2$. *Let* $P_{A_f}(x)$ *denote the number the primes* $p \le x$ *for which* A_f *is not ordinary at* p. *There exists a constant* $c_f > 0$ *such that*

$$P_{A_f}(x) \sim c_f \log\log x \quad \text{as } x \to \infty.$$

9. NUMERICAL EXAMPLES

We give in Table 1 the distribution of the values $r_p(X_0(l))$ for primes $l < 100$ and $p < 10^3$. It is obtained by using the tables of the characteristic polynomials of the Hecke operators T_p computed by Wada. The entries in the headed column g give the genus of $X_0(l)$, and n the number of isogeny classes of $\mathbb{Q}$-defined modular elliptic curves of conductor l. The entries in columns $r_p = i$ give the number of primes $p < 10^3$ for which $r_p(X_0(l)) = i$. The entries in columns $r_p < g$ display the whole number of nonordinary reductions in the range. We note that if $f \in S_2(\Gamma_0(l))$ is a newform, then A_f is absolutely simple and $\mathbb{Q} \otimes \operatorname{End}(A_f)$ is a commutative field; thus, $d = \dim A_f$.

For $x = 10^3$, the functions $\sqrt{x}/\log x$, $\log\log x$ take the values 4.58 and 1.93 respectively. In Table 1, in all levels for which the frequency of nonordinary reductions is ≥ 5, we find a $\mathbb{Q}$-defined modular elliptic curve of conductor l. If the frequency is > 10, then there are two isogeny classes of such curves. In contrast, in levels with frequency ≤ 3, there are no elliptic modular curves of this conductor.

In Table 2, A denotes the abelian variety $J_0(l)$ deprived of its modular elliptic factors, for $l \le 100$. In its columns, n denotes the number of isogeny classes of the $\mathbb{Q}$-simple subvarieties $A_f = B_f$ of A, and d their respective dimensions. We list the values $P_B(10^3)$, $P_B(10^4)$, $P_{B,0}(10^3)$, $P_{B,0}(10^4)$ when B runs through the set of isogeny classes of $\mathbb{Q}$-simple subvarieties of A. The table has been computed from the characteristic polynomials of the Hecke operators T_p, $p < 10^4$, supplied to us by Wang.

The function log log increases so slowly that it is a time-consuming process to build trust in the conjectures. Nevertheless, the numerical results support them in the given range. Indeed, if $m(x)$ denotes the arithmetical mean of the values $P_B(x)$ for the 20 subvarieties B in Table 2, we have

$$\frac{m(10^4)}{m(10^3)} = \frac{33/20}{24/20} = 1.375,$$

whereas

$$\frac{\log(\log(10^4))}{\log(\log(10^3))} = 1.149.$$

Note that, in Table 2, we have only five subvarieties B for which is $P_{B,0}(10^4) > 0$. For $l \ne 97$, we have $\dim B = 2$. The cases correspond to the levels

l	g	$r_p=0$	$r_p=1$	$r_p=2$	$r_p=3$	$r_p=4$	$r_p=5$	$r_p=6$	$r_p=7$	$r_p<g$	n
11	1	6	161							6	1
17	1	5	162							5	1
19	1	7	160							7	1
23	2	2	0	165						2	0
29	2	0	0	167						0	0
31	2	0	0	167						0	0
37	2	1	10	156						11	2
41	3	0	0	0	167					0	0
43	3	1	0	3	163					4	1
47	4	0	0	0	0	167				0	0
53	4	0	0	0	6	161				6	1
59	5	0	0	1	0	0	166			1	0
61	4	0	0	0	4	163				4	1
67	5	0	0	0	0	10	157			10	1
71	6	0	0	0	0	1	2	164		3	0
73	5	0	0	0	2	6	159			8	1
79	6	0	0	0	0	0	7	160		7	1
83	7	0	0	0	0	1	0	9	157	10	1
89	7	0	0	0	0	0	1	11	155	12	2
97	7	0	0	0	0	1	0	3	163	4	0

TABLE 1. Distribution of $r_p(X_0(l))$ for primes $l<100$ and $p<10^3$.

$A=J_0(l)/E_i$	$\dim A$	n	d	$P_B(10^3)$	$P_B(10^4)$	$P_{B,0}(10^3)$	$P_{B,0}(10^4)$
$J_0(23)$	2	1	2	2	3	2	3
$J_0(29)$	2	1	2	0	0	0	0
$J_0(31)$	2	1	2	0	0	0	0
$J_0(41)$	3	1	3	0	0	0	0
$J_0(43)/E_{43A}$	2	1	2	2	2	1	1
$J_0(47)$	4	1	4	0	1	0	0
$J_0(53)/E_{53A}$	3	1	3	1	1	0	0
$J_0(59)$	5	1	5	1	1	0	0
$J_0(61)/E_{61A}$	3	1	3	0	0	0	0
$J_0(67)/E_{67A}$	4	2	2, 2	1, 1	1, 1	0, 0	0, 0
$J_0(71)$	6	2	3, 3	2, 2	4, 2	0, 0	0, 0
$J_0(73)/E_{73B}$	4	2	2, 2	3, 1	3, 2	1, 0	1, 1
$J_0(79)/E_{79A}$	5	1	5	1	1	0	0
$J_0(83)/E_{83A}$	6	1	6	2	3	0	0
$J_0(89)/(E_{89A}\times E_{89C})$	5	1	5	1	1	0	0
$J_0(97)$	7	2	3, 4	2, 2	4, 3	1, 0	1, 0

TABLE 2. Data on the the quotient variety A of $J_0(l)$ by its modular elliptic factors, and on the classes of $\mathbb{Q}$-simple subvarieties of A.

$l = 23$ and $p = 43, 109, 1033$; $l = 43$ and $p = 2$; and $l = 73$ and $p = 59, 1117$. In the twelve remaining cases with $\dim B > 2$, we find only a newform f and a prime p for which $r_p(A_f) = 0$. This happens in level $l = 97$ and $p = 7$; furthermore, since the characteristic polynomial of T_7 is $x^3+7x^2+14x+7$, we see that $a(7) \neq 0$.

If $m_0(x)$ denotes the arithmetical mean of the values $P_{B,0}(x)$ for the eight subvarieties B of dimension 2 in Table 2, we have

$$\frac{m_0(10^4)}{m_0(10^3)} = \frac{6/8}{4/8} = 1.5.$$

The growth of $m_0(x)$ in the range is reasonably similar to that of $m(x)$ and $\log\log x$.

In Table 3 we show the Hasse–Witt invariants of $A_N := J_1(N)/J_0(N)$, for $N < 31$, $p < 100$. The table is obtained by using the characteristic polynomials of the Hecke operators T_p calculated by Lario. Here g denotes the dimension of A_N.

For $N = 20, 21, 24, 28$ we have many nonordinary primes, since $13 \leq P_{A_N}(100) \leq 15$. This is due to the fact that, at these levels, there is a newform generating a rational subspace of dimension 2 that has complex multiplication. Indeed, let K be one of the imaginary quadratic fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, and let $\mathfrak{m}$ be the integral ideal $(2+i)$, $(2+\sqrt{-3})$, $(1+\sqrt{-2})$, $((1/2+\sqrt{-7}/2)^2)$, respectively. The discriminant $-D$ is equal to -4, -3, -8, -7, respectively, and the norm M of $\mathfrak{m}$ is 5, 7, 3, 4, respectively. The integer ring $\mathcal{O}$ of K is a principal ideal domain. Each integral ideal $\mathfrak{a}$ prime to $\mathfrak{m}$ has one and only one basis $z_{\mathfrak{a}}$ such that $z_{\mathfrak{a}} \equiv 1 \pmod{\mathfrak{m}}$. This is due to the fact that two different roots of unity in $\mathcal{O}$ have different classes mod $\mathfrak{m}$ and that the set of classes mod $\mathfrak{m}$ of roots of unity in $\mathcal{O}$ coincides with the group $(\mathcal{O}/\mathfrak{m}\mathcal{O})^* \simeq (\mathbb{Z}/M\mathbb{Z})^*$. Hence, the formula $\psi(\mathfrak{a}) = z_{\mathfrak{a}}$ defines a Grössencharakter mod $\mathfrak{m}$ of K. Thus, there exists a parabolic form of weight 2 with complex multiplication for $\Gamma_1(DM)$. Moreover, it is easy to prove that the level of this form is $DM = N$.

For $N = 26, 30$, we have $5 \leq P_{A_N}(100) \leq 8$. If $N = 26$, then $J_1(26)/J_0(26)$ is $\mathbb{Q}$-isogenous to $A_{f_1} \times A_{f_2} \times A_{f_3}^2$, where f_1, f_2 are newforms of level 26, and f_3 is a newform of level 13. Moreover, each A_{f_i} is $\bar{\mathbb{Q}}$-isogenous to the square of a simple abelian variety B_{f_i} of dimension 1. If $N = 30$, then $J_1(30)/J_0(30)$ is $\mathbb{Q}$-isogenous to $A_{f_1} \times A_{f_2}$, where f_1, f_2 are newforms of level 30. We have $A_{f_i} \sim B_{f_i}^2$ for $i = 1, 2$, $F = \mathbb{Q}$, but $\dim B_{f_1} = 1$, $\dim B_{f_2} = 2$. Observe that the Hasse–Witt invariants of $J_1(26)/J_0(26)$ behave like those of $\mathcal{C}_1^2 \times \mathcal{C}_2^2 \times \mathcal{C}_3^4$, and the Hasse–Witt invariants of $J_1(30)/J_0(30)$ behave like those of $\mathcal{C}_1^2 \times \mathcal{C}_2^4$; here the $\mathcal{C}_i$ denote elliptic curves over $\mathbb{Q}$.

For $N = 13, 16, 18$, we have $1 \leq P_{A_N}(100) \leq 2$. In these cases, $A_N = A_f \sim B_f^2$ with $\dim B_f = 1$. In the remaining cases is $P_{A_N}(100) = 0$, and A_N has no subvarieties A_f for which $F = \mathbb{Q}$.

ACKNOWLEDGEMENTS

We are grateful to G. Frey, H. Rück and J.-P. Serre for their help in a preliminary study of these questions and to J. C. Lario and X. Wang for kindly providing us with extensive tables of characteristic polynomials of Hecke operators. The authors also thank the referees for valuable comments on an earlier version of this paper.

REFERENCES

[de Shalit 1987] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication; p-adic L functions*, Perspectives in Mathematics **3**, Academic Press, Boston, 1987.

[Deligne et al. 1982] P. Deligne, J. S. Milne, A. Ogus, and K.-Y. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Math. **900**, Springer, Berlin, 1982.

[Deuring 1941] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.

[Elkies 1987] N. D. Elkies, "The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$", *Invent. Math.* **89**:3 (1987), 561–567.

$N =$	13	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$g =$	2	2	4	2	6	2	4	4	10	4	12	8	12	8	20	6
p	r_p															
2	2	–	4	–	6	–	0	–	10	–	12	–	12	–	20	–
3	2	2	4	–	6	0	–	4	10	–	12	6	–	2	20	–
5	2	2	4	0	6	–	2	4	10	2	–	8	12	6	20	–
7	0	2	4	2	6	0	–	4	10	2	12	4	12	–	20	6
11	0	2	4	2	6	0	2	–	10	2	12	2	12	8	20	6
13	–	2	4	2	6	2	4	4	10	2	12	–	12	6	20	2
17	2	2	–	2	6	2	0	4	10	4	12	8	12	6	20	6
19	2	2	4	2	–	0	4	4	10	4	12	6	12	6	18	4
23	2	2	4	2	6	0	0	4	–	2	12	8	12	8	20	6
29	2	2	4	2	6	2	2	4	10	2	12	6	12	8	–	4
31	2	2	4	2	6	0	4	4	10	2	12	6	12	6	20	6
37	2	2	4	2	6	2	4	4	10	2	12	8	12	8	18	6
41	2	0	4	2	6	2	2	4	10	4	12	6	12	6	20	6
43	2	2	4	2	6	0	4	4	10	4	12	8	12	8	20	6
47	2	2	4	2	6	0	2	4	10	2	12	8	12	6	20	2
53	2	2	4	2	6	2	2	4	10	2	12	8	12	8	20	6
59	2	2	4	2	6	0	2	4	10	4	12	8	12	6	20	6
61	2	2	4	2	6	2	4	4	10	0	12	8	12	6	20	6
67	2	2	4	2	6	0	4	4	10	4	12	8	12	8	20	6
71	2	2	4	2	6	0	2	4	10	2	12	8	12	6	16	6
73	2	2	4	2	6	2	4	4	10	4	12	8	12	6	18	6
79	2	0	4	2	6	0	4	4	10	2	12	8	12	8	20	4
83	2	2	4	2	6	0	2	4	10	4	12	6	12	6	20	6
89	2	2	4	2	6	2	2	4	10	4	12	8	12	6	20	6
97	2	2	4	2	6	2	4	4	10	4	12	8	12	6	20	6

TABLE 3. Hasse–Witt invariants of $A_N := J_1(N)/J_0(N)$.

[Elkies 1991] N. D. Elkies, "Distribution of supersingular primes", pp. 127–132 in *Journées Arithmétiques* (Luminy, 1989), Astérisque **198-200**, Soc. math. France, Montrouge, 1991.

[González 1997] J. González, "Hasse–Witt matrices for the Fermat curves of prime degree", *Tohoku Math. J.* **49** (1997).

[Gonzàlez Rovira 1991] J. Gonzàlez Rovira, "Equations of hyperelliptic modular curves", *Ann. Inst. Fourier* (*Grenoble*) **41**:4 (1991), 779–795.

[Hasse 1934] H. Hasse, "Existenz separabler zyklischer unverzweigter Erweiterungskörpern vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p", *J. Reine angew. Math.* **172** (1934), 77–85.

[Hasse and Witt 1936] H. Hasse and E. Witt, "Zyklische unverzweigte Erweiterungskörpern vom Primzahlgrade p über einem algebraischen Funktionenkörpern der Charakteristik p", *Monats. Math. Phys.* **43** (1936), 477–492.

[Hecke 1981] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Math., Springer, New York, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[Huppert 1967] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften **134**, Springer-Verlag, Berlin, 1967.

[Lang and Trotter 1976] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*, Lecture Notes in Math. **504**, Springer, Berlin, 1976.

[Manin 1961] J. I. Manin, "The Hasse-Witt matrix of an algebraic curve", *Izv. Akad. Nauk SSSR Ser. Mat.* **25** (1961), 153–172. In Russian. Translated in *Amer. Math. Soc. Transl. Ser.* **45** (1965), 245–264.

[Manin 1962] J. I. Manin, "On the theory of Abelian varieties over a field of finite characteristic", *Izv. Akad. Nauk SSSR Ser. Mat.* **26** (1962), 281–292. In Russian.

[Momose 1981] F. Momose, "On the l-adic representations attached to modular forms", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**:1 (1981), 89–109.

[Ribet 1977] K. A. Ribet, "Galois representations attached to eigenforms with Nebentypus", pp. 17–51 in *Modular functions of one variable V* (Bonn, 1976), Lecture Notes in Math. **601**, Springer, Berlin, 1977.

[Ribet 1980] K. A. Ribet, "Twists of modular forms and endomorphisms of abelian varieties", *Math. Ann.* **253**:1 (1980), 43–62.

[Ribet 1985] K. A. Ribet, "On l-adic representations attached to modular forms II", *Glasgow Math. J.* **27** (1985), 185–194.

[Ribet 1992] K. A. Ribet, "Abelian varieties over $\mathbb{Q}$ and modular forms", pp. 53–79 in *Algebra and topology* (Taejŏn, Korea, 1992), edited by S. G. Hahn and D. Y. Suh, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[Ribet 1994] K. A. Ribet, "Fields of definition of abelian varieties with real multiplication", pp. 107–118 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994.

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. Reprinted in Œuvres, vol. 3, Springer, 1986.

[Serre 1985/86] J.-P. Serre, "Résumés des cours au Collège de France", *Annuaire du Collège de France* (1985/86), 95–99.

[Serre 1989] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute.

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, Princeton University Press and Iwanami Shoten, Tokyo, 1971.

[Tate 1965] J. T. Tate, "Algebraic cycles and poles of zeta functions", pp. 93–110 in *Arithmetical Algebraic Geometry* (Purdue Univ., 1963), edited by O. F. G. Schilling, Harper & Row, New York, 1965.

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144.

Pilar Bayer, Facultat de Matemàtiques, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, E-08007 Barcelona, Spain (bayer@cerber.mat.ub.es)

Josep González, Escola Universitària Politècnica de Vilanova i la Geltrú, av. Víctor Balaguer s/n, E-08800 Vilanova i la Geltrú, Spain (josepg@mat.upc.es)

Received January 18, 1995; revision received July 12, 1996; accepted October 2, 1996