# On the Manin constants of modular elliptic curves

Bas Edixhoven

December 24, 1998

## 1 Definitions and results

For $M$ a positive integer, let $X_0(M)_{\mathbf{Q}}$ be the modular curve over $\mathbf{Q}$ classifying elliptic curves with a given cyclic subgroup of order $M$ and let $J_0(M)_{\mathbf{Q}}$ be the jacobian of $X_0(M)_{\mathbf{Q}}$. An elliptic curve $E$ over $\mathbf{Q}$ is said to be *modular* if it is an isogeny factor (isogenies over $\mathbf{Q}$) of some $J_0(M)_{\mathbf{Q}}$; the smallest $M$ for which this happens is then called the level of $E$. The Shimura-Taniyama conjecture states that *every* elliptic curve $E$ over $\mathbf{Q}$ is modular, and that the level of $E$ equals the conductor of $E$. A modular elliptic curve of level $M$ is called *strong* if there exists a closed immersion $E \hookrightarrow J_0(M)_{\mathbf{Q}}$. It follows from the multiplicity one principle for modular forms that such an immersion is unique up to sign.

Let $E$ be a strong modular elliptic curve of level $M$. The corresponding *strong modular parametrization* $\phi : X_0(M)_{\mathbf{Q}} \to E$ is obtained as follows:

$$\begin{array}{ccc} J_0(M)_{\mathbf{Q}} & \to & E \\ \uparrow & \nearrow_{\phi} & \\ X_0(M)_{\mathbf{Q}} & & \end{array}$$

where $J_0(M)_{\mathbf{Q}} \to E$ is the dual of one of the two closed immersions $E \hookrightarrow J_0(M)_{\mathbf{Q}}$ and where $X_0(M)_{\mathbf{Q}} \to J_0(M)_{\mathbf{Q}}$ is the standard immersion sending the cusp $\infty$ to 0. Let $\mathcal{E}$ be the Néron model over $\mathbf{Z}$ of $E$. Then the $\mathbf{Z}$-module of translation invariant differentials on $\mathcal{E}$ is free of rank one; let $\omega$ be one of the two generators. We get the differential form $\phi^*\omega$ on $X_0(M)_{\mathbf{Q}}$. Now there is also a second differential form on $X_0(M)_{\mathbf{Q}}$ related to $E$: the normalized newform $\sum a_n q^n \frac{dq}{q}$ corresponding to $E$ (normalized means that $a_1 = 1$). The multiplicity one principle gives:

$$\phi^*\omega = c \sum_{n\geq 1} a_n q^n \frac{dq}{q}$$

for some $c \in \mathbf{Q}^*$. This number $c$ is called the Manin constant of $E$ (see [7], [8], [9] and [1]).

**Conjecture 1 (Manin)** *$c = \pm 1$.*

In [7] Mazur showed that $c \in \mathbf{Z}[\frac{1}{2m}]^*$, where $m$ is the largest square dividing $M$. His proof uses results of Raynaud on specialization of finite group schemes (this explains why 2 plays a special rôle) and the description of Deligne and Rapoport [3] of the reduction of $X_0(M)_{\mathbf{Q}}$ over $\mathbf{Z}[\frac{1}{m}]$. The fact that $X_0(M)_{\mathbf{Q}}$ has stable reduction over $\mathbf{Z}[\frac{1}{m}]$ is crucial. It seems [14] [10] that in a letter to Mestre (Febr. 1985), Raynaud has stated general results implying that, for 2 not dividing $m$, one has $v_2(c) = 0$ or 1, where $v_2(c)$ is the valuation of $c$ at 2. In this article we will be concerned with the primes $p$ dividing $m$. First we prove the following proposition.

**Proposition 2** *The number $c$ is an integer.*

*Proof.* Let $X_0(M)$ be the compactified coarse moduli scheme $\overline{\mathrm{M}}([\Gamma_0(M)])$ (cf. [6] (8.6)). Let $X_0(M)^0$ be the open part of $X_0(M)$ where the projection to $\mathrm{Spec}(\mathbf{Z})$ is smooth. Let $\mathcal{E}$ be the Néron model of $E$ over $\mathbf{Z}$. By the Néron property $\phi$ extends to $\phi : X_0(M)^0 \longrightarrow \mathcal{E}$. It follows immediately from [6] Thm.8.11.10 that the formal completion of $X_0(M)$ along the (unramified) cusp $\infty$ is $\mathrm{Spf}(\mathbf{Z}[[q]])$. We see that $\infty \in X_0(M)^0(\mathbf{Z})$ and that $\phi^*\omega_{\mathbf{Z}}$ is a differential form (without poles!) in a neighborhood of $\infty$. If $c$ would not be integral, then $\phi^*\omega_{\mathbf{Z}}$ would have poles along the fibers of $X_0(M)^0$ in characteristics dividing the denominator of $c$.

The analogous result for parametrizations involving the modular curve $X_1(M)$ is proved in the paper [14] by Stevens. In that paper Stevens studies parametrizations of Weil curves by the modular curves $X_1(M)$. He conjectures (see [14] Conj. I) that *every* Weil curve $E$ (not just the strong ones) admits a parametrization by $X_1(M)$ (where $M$ is the conductor of $E$) with Manin constant equal to 1. He shows this conjecture to be compatible with quadratic twists over fields that are unramified at the primes where $E$ has additive reduction. He also shows, using results of Rubin on special values of $L$-functions, that a weak form of his conjecture holds for certain elliptic curves with complex multiplication.

Using the classification by Mazur [7] of the rational torsion points of elliptic curves over $\mathbf{Q}$, one can easily show that up to the primes 2, 3, 5, and 7, Stevens's version of Manin's conjecture is equivalent to Manin's conjecture. For this one remarks that the difference between parametrizations by $X_1(M)_{\mathbf{Q}}$ and $X_0(M)_{\mathbf{Q}}$ lies in the so-called Shimura subgroup of $J_0(M)_{\mathbf{Q}}$, which is the Cartier dual of a constant group. It follows that the Manin constant $c$ of a strong Weil curve $E$ is not divisible by primes $p > 7$ where $E$ has reduction type $I_0^*$ or $I_\nu^*$ (we use Kodaira symbols to denote the possible reduction types of elliptic curves, see [15]).

The aim of this article is to attack Manin's conjecture for the remaining reduction types, these are: $II$, $III$, $IV$, $IV^*$, $III^*$ and $II^*$. Our method to do this is in principle the same as Mazur's [7]: to study the valuation of $c$ at a prime $p$ by reducing $\phi$ modulo $p$. As remarked above, it is crucial to have stable models for $X_0(M)$ and $E$ at $p$. This makes it necessary not to work with the model of $X_0(M)$ over $\mathbf{Z}$ as constructed in [6], but over a suitable extension of $\mathbf{Q}$ over which $X_0(M)$ and $E$ acquire stable reduction. For a number of reasons, we suppose that $p > 7$. It has been proved by Carayol [2], that for modular elliptic curves the level and the conductor coincide. The conductors of the curves that we want to study are of the form $p^2N$, where $p$ does not divide $N$. A stable model of $X_0(p^2N)$ at $p$ is constructed in [4]. The application of these stable models to the study of Manin constants is given in [5] 4.6. The result that we state here is slightly stronger than [5] Thm.4.6.3.

**Theorem 3** *Let $\phi : X_0(M)_{\mathbf{Q}} \to E$ be a strong modular parametrization, let $c$ be its Manin constant and let $p > 7$ be a prime. Then $p$ does not divide $c$, except possibly when $E$ has potentially ordinary reduction at $p$ of type $II$, $III$ or $IV$. In that case, $p$ divides $c$ at most once.*

Of course, the cases where $E$ has reduction type $I_0$, $I_\nu$, $I_0^*$ or $I_\nu^*$ are already proved by Mazur and Stevens. In the proof of the theorem for curves with complex multiplication we rely heavily on the work of Stevens. Combining our results with those of Stevens on complex multiplication curves, one can even show that elliptic curves over $\mathbf{Q}$ with complex multiplication by $\mathbf{Q}(\sqrt{-p})$, $p>3$, have Manin constants (in the original sense as well as in the sense of Stevens) equal to 1 or 2. A lot of details of the proof of the theorem above are not given here; for them we refer to [5]. Finally I want to thank Ling San for giving his comments on a preliminary version of this article.

# 2 Stable models

The standard method to try to obtain a stable model of a curve over the spectrum $S$ of a discrete valuation ring is as follows. One starts with a regular model $X$ over $S$. After blowing up repeatedly in closed points of the special fibre one may assume $X$ is a regular model in which the special fibre is a divisor with normal crossings. Now let $n$ be the least common multiple of the multiplicities in this divisor and let $\pi_0$ be a uniformizer on $S$. Let $T$ be $S[\pi]$, with $\pi^n=\pi_0$, thus we have $T\to S$ totally ramified of degree $n$. Let $\widetilde{X_T}$ be the normalization of the pullback $X_T$ of $X$ to $T$. Let $t$ be the closed point of $T$. If $n$ is invertible on $S$, then by easy explicit computations with the complete local rings of $X$, one can show that $\widetilde{X_T}$ is a stable model in the sense that the only singularities of $X_t$ are ordinary double points.

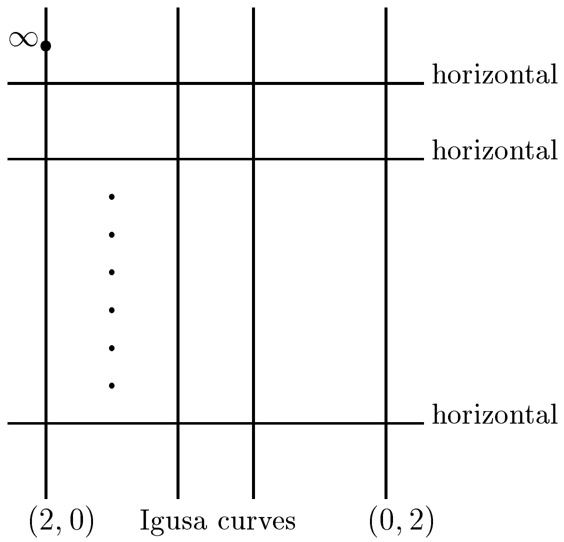
Now suppose that $n$ is invertible on $S$ and that $\mathcal{O}_S(S)$ contains $\mu_n$, the $n$-th roots of unity. Then $\mu_n$ acts on $T$ by:

$$\forall\zeta\in\mu_n:\qquad \zeta^{\#}:\pi\mapsto\zeta\pi,$$

where $\zeta^{\#}$ is the automorphism of $\mathcal{O}_T$ corresponding to the automorphism $\zeta$ of $T$. The quotient for this action is the morphism $T\to S$. We let $\mu_n$ act on $X_T=X\times_S T$ via its action on $T$. It follows that $\mu_n$ also acts on its normalization $\widetilde{X_T}$. Since the morphism $\widetilde{X_T}\to T$ is equivariant and $t$ is fixed (i.e., $\mu_n$ acts trivially on $k(t)$), $\mu_n$ acts $k(t)$-linearly on the special fibre $\widetilde{X_{T,t}}$. The $\mu_n$-action on the complete local rings of $\widetilde{X_{T,t}}$ is easy to compute.

We will now apply the method described above to the modular curve $X_0(p^2N)$. Let $p>3$ be a prime, and let $N$ be a positive integer that is not divisible by $p$. We start with the model over $\mathbf{Z}$ as contructed by Katz and Mazur in [6] 8.6. In their terminology, we let $X_0(p^2N)$ be the coarse compactified moduli scheme over $\mathbf{Z}$ associated to the moduli problem $\Gamma_0(p^2N)$.

Figure 1: The stable reduction of $X_0(p^2N)$ at $p$.




Let $S$ be the spectrum of the ring of Witt vectors of $\overline{\mathbf{F}}_p$, and let $X_0(p^2N)_S$ be the pullback of $X_0(p^2N)$ to $S$. Then $X_0(p^2N)_S$ is a curve over $S$ with a smooth geometrically irreducible generic fibre. The two-dimensional scheme $X_0(p^2N)$ is regular, except for some possible quotient singularities. There are two ways to get rid of these singularities. One way is to work with the minimal resolution of $X_0(p^2N)$ (see [4]). The other way is to introduce a suitable additional level structure (e.g., $[\Gamma(3)^{\mathrm{can}}]$); then to apply the method described above to the associated moduli scheme, and to obtain the stable model of $X_0(p^2N)$ as a quotient. The details of this computation can be found in [4]. It turns out that $X_0(p^2N)_S$ acquires stable reduction over $T = S[\pi]$, with $p = \pi^n$ and $n = \frac{p^2-1}{2}$. We denote the stable model by $\widetilde{X_T}$. The details of the computation of the action of $\mu_n$ on $\widetilde{X_{T,t}}$ can be found in [5]. The description that one finds of $\widetilde{X_{T,t}}$ together with its $\mu_n$-action is as follows. Figure 1 contains a picture of $\widetilde{X_{T,t}}$.

The outer two vertical components are the (2,0) and (0,2) components (in the terminology of [6]) from $X_0(p^2N)_s$. These curves are both isomorphic to $X_0(N)_s$, where $s$ denotes the closed point of $S$. The two central vertical components are isomorphic to the curve $\overline{\mathrm{M}}([\Gamma_0(N)], [Ig(p)/\{\pm 1\}])$ (see [6] 12 for the details of the Igusa moduli problem). The supersingular points on the central vertical components correspond bijectively to the supersingular points on $X_0(N)_s$. The four vertical components are glued to the horizontal components at their supersingular points. The horizontal component corresponding to a supersingular point $x$ of $X_0(N)_s$ is the smooth complete hyperelliptic curve given by the equation:

$$y^2 = x^{p+1} + 1,$$

if the automorphism group of $x$ is $\{\pm 1\}$ (by this we mean that the pair $(E, G)$, corresponding to $x$ via the moduli interpretation, has automorphism group $\{\pm 1\}$). In general, the horizontal component at $x$ is the quotient of this curve by some action of $\mathrm{Aut}_s(x)$. Each horizontal component is glued to the outer two vertical components at the points with $x = \infty$, $y = \infty$. At the points $x = 0$, $y = \pm 1$ it is glued to the central vertical components.

The inertia group $\mu_n$ preserves the horizontal components; the action on each horizontal component is given by:

$$\forall \zeta \in \mu_n : \qquad \zeta^{\#} : \begin{cases} x & \mapsto & \zeta^{-\frac{p-1}{2}} x \\ y & \mapsto & \zeta^{\frac{n}{2}}. \end{cases}$$

The $\mu_n$-action on the vertical components is as follows. The action is trivial on the outer two components. The two Igusa curves are interchanged. The stabilizer of either of them, $\mu_{\frac{n}{2}}$, acts on the Igusa curve via its action on the moduli problem $[Ig(p)/\{\pm 1\}]$.

From this description, it is easy to make a list of all the points in $\widetilde{X_{T,t}}$ that are stabilized by $\mu_{\frac{n}{2}}$, together with the $\mu_{\frac{n}{2}}$-actions on the cotangent spaces at those points. This list is very useful in the study of the differential forms on $\widetilde{X_{T,t}}$.

Since we want to study modular parametrizations of elliptic curves by looking at their stable reductions, we have to study the stable reduction of elliptic curves too. This is done by the same method that we used for the modular curves. The results of these computations are summarized in the following proposition.

**Proposition 4** *Let $S$ be the spectrum of a complete discrete valuation ring, with algebraically closed residue field not of characteristic 2 or 3. Let $E$ be an elliptic curve over the generic point of $S$. We attach a number $n$ and* *a character $\chi_\omega : \mu_n \to \mu_n$ to $E$ according to its reduction type as follows ($\chi : \mu_n \to \mu_n$ denotes the identity):*

| type | $I_0$ | $I_\nu$ | $II$ | $III$ | $IV$ | $I_0^*$ | $I_\nu^*$ | $IV^*$ | $III^*$ | $II^*$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | 1 | 1 | 6 | 4 | 3 | 2 | 2 | 3 | 4 | 6 |
| $\chi_\omega$ | $\chi$ | $\chi$ | $\chi$ | $\chi$ | $\chi$ | $\chi$ | $\chi$ | $\chi^{-1}$ | $\chi^{-1}$ | $\chi^{-1}$ |

*Let $\pi_0$ be a uniformizer on $S$. Then $E$ acquires stable reduction over $T := S[\pi]$, where $\pi^n = \pi_0$. The Galois group of $T$ over $S$ is identified with $\mu_n$ by: $\zeta^\# \pi = \zeta\pi$ for all $\zeta \in \mu_n$. Let $t$ be the closed point of $T$ and $\widetilde{\mathcal{E}_T}$ the Néron model of $E_T$. The the action of $\mu_n$ on the tangent space at $0$ of $\widetilde{\mathcal{E}_{T,t}}$ is given by $\chi_\omega$.*

# 3 Modular parametrizations

Let $\phi : X_0(p^2N) \to E$ be a strong modular parametrization where $p > 3$ is a prime that does not divide the positive integer $N$. We suppose that $E$ has potentially good reduction at $p$ (this means that we exclude the reduction type $I_\nu^*$). Let $S := \operatorname{Spec} W(\overline{\mathbf{F}}_p)$, $n := \frac{p^2-1}{2}$, $U := S[\pi]$, where $\pi^n = p$. In the previous section we have seen that both $X_0(p^2N)$ and $E$ acquire stable reduction over $U$. We denote these stable models by $\widetilde{X_U}$ and $\widetilde{\mathcal{E}_U}$, respectively. The parametrization $\phi$ gives, by pullback, a morphism (still denoted $\phi$) between the generic fibres of $\widetilde{X_U}$ and $\widetilde{\mathcal{E}_U}$.

**Proposition 5** *This $\phi$ extends to a morphism $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$.*

*Proof.* This follows from the facts that $\widetilde{\mathcal{E}_U}$ is an abelian scheme and $\widetilde{X_U}$ a stable curve.

The fact that the map $\phi : \widetilde{X_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ (where $u$ denotes the closed point of $U$) is $\mu_n$-equivariant already gives a lot of information. For example, let us consider the orders of the $\mu_n$-action on the various components of $\widetilde{X_{U,u}}$: on a horizontal component, this order divides $p+1$; on the two outer vertical components it is 1 and on the two central vertical components together, it is $p-1$. Let $d$ be the order of the $\mu_n$-action on $\widetilde{\mathcal{E}_{U,u}}$ (see the table in proposition 4). It follows that all the components of $\widetilde{X_{U,u}}$ on which the order of the $\mu_n$-action is not divisible by $d$ will be contracted by $\phi$. This leads us to the following proposition.

**Proposition 6** *The morphism $\phi : \widetilde{X_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ is constant on the two outer vertical components. On the other components we have:*

| type | $p$ | hor. components | central vert. comps. |
|---|---|---|---|
| $I_0^*$ | | contracted | |
| $II, IV, IV^*, II^*$ | $p \equiv 1(3)$ | contracted | |
| | $p \equiv -1(3)$ | | contracted |
| $III, III^*$ | $p \equiv 1(4)$ | contracted | |
| | $p \equiv -1(4)$ | | contracted |

*Remark.* In order to prove that each horizontal component $C$ is contracted in the case where $E$ has reduction type $I_0^*$, one has to use that the quotient of $C$ by $\mu_{\frac{n}{2}}$ has genus 0.

The remainder of this section will be concerned with the degree of inseparability of $\phi : \widetilde{X_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$. The next proposition shows that there will always be at least one component of $\widetilde{X_{U,u}}$ on which $\phi$ is either separable or the composition of a separable morphism with the Frobenius endomorphism of $\widetilde{\mathcal{E}_{U,u}}$. Let $\widetilde{J_U}^0$ denote the connected component of the Néron model of $J_0(p^2N)$ over $U$. Since $\widetilde{X_U}$ is a stable curve, $\widetilde{J_U}^0$ is the Picard scheme $\mathrm{Pic}^0_{\widetilde{X_U}/U}$ (see [12] 6.1.4, 6.1.6 and 8.2.1).

**Proposition 7** *Let $G$ be the kernel of $\phi^* : \widetilde{\mathcal{E}_{U,u}} \to \widetilde{J_{U,u}}^0$. If $p > 7$, then either $G = 0$ or $G = \ker(V : \widetilde{\mathcal{E}_{U,u}} \to \widetilde{\mathcal{E}_{U,u}})$, the kernel of the Verschiebung.*

*Proof.* Since $\phi : X_0(p^2N)_{\mathbf{Q}} \to E$ is strong, we have that $\phi^* : \widetilde{\mathcal{E}_U} \to \widetilde{J_U}^0$ is injective on the generic fibre. It follows from the semistability of $\widetilde{\mathcal{E}_U}$ and $\widetilde{J_U}^0$ that $G$ is finite and consists of $p$-power torsion. Now we want to apply a result of Raynaud on the specialization of finite group schemes [13] Corollaire 3.3.6.1

(see also [7] Proposition 1.1) to study the kernel of $\phi^* : \widetilde{\mathcal{E}_U} \to \widetilde{J_U}^0$. We can not use this result of Raynaud directly, because the absolute ramification index of $U$ is $n = \frac{p^2-1}{2} \geq p-1$.

Therefore let $T \to S$ be the minimal base change such that $E$ acquires good reduction (see proposition 4, hence $T \to S$ is of degree 2, 3, 4 or 6). Taking the quotient of $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$ by the action of the subgroup $\mathrm{Gal}(U/T)$ of $\mu_n$ gives us a morphism $\phi : \widetilde{X_T} \to \widetilde{\mathcal{E}_T}$. By Picard functoriality we get: $\phi^* : \widetilde{\mathcal{E}_T} \to \widetilde{J_T}^0$, where $\widetilde{J_T}^0$ is defined to be $\mathrm{Pic}^0_{\widetilde{X_T}/T}$ ($\mathrm{Pic}^0_{\widetilde{X_T}/T}$ is representable by a smooth group scheme by [12] 8.2.1, we do not know whether $\mathrm{Pic}^0_{\widetilde{X_T}/T}$ is the Néron model). Since the absolute ramification index of $T$ is less than $p-1$ (this explains the hypothesis "$p > 7$" in this proposition), we can now apply the result of Raynaud mentioned above to $\phi^* : \widetilde{\mathcal{E}_T}[p] \to H$, where $H$ is the image of $\widetilde{\mathcal{E}_T}[p]$ in $\widetilde{J_T}^0$. The conclusion is that $\phi^* : \widetilde{\mathcal{E}_T} \to \widetilde{J_T}^0$ is a closed immersion.

By pullback to $U$ we get a commutative diagram:

$$\begin{array}{ccc} \widetilde{\mathcal{E}_{T,U}} & \hookrightarrow & \widetilde{J_{T,U}}^0 \\ \downarrow & & \downarrow \\ \widetilde{\mathcal{E}_U} & \to & \widetilde{J_U}^0 \end{array}$$

where $\widetilde{\mathcal{E}_{T,U}} \to \widetilde{\mathcal{E}_U}$ is an isomorphism (since $E$ has already good reduction over $T$) and where $\widetilde{J_{T,U}}^0 \to \widetilde{J_U}^0$ exists because of the Néron property of $\widetilde{J_U}^0$. It follows that:

$$G = \widetilde{\mathcal{E}_{T,t}} \cap \ker(\widetilde{J_{T,t}}^0 \to \widetilde{J_{U,u}}^0).$$

Using our knowledge of $\widetilde{X_T}$ and $\widetilde{X_U}$ it is not hard to show that $\ker(\widetilde{J_{T,t}}^0 \to \widetilde{J_{U,u}}^0)$ is purely additive: it is isomorphic to a direct sum of $\mathbf{G}_{a,t}$'s. The reason that this is true is that the multiplicities of the irreducible components in $\widetilde{X_{T,t}}$ are less than $p$ (from this it follows that there is an exponential sequence).

It remains to find out what the intersection of $\widetilde{\mathcal{E}_{T,t}}$ with a direct sum of additive groups can be. If $\widetilde{\mathcal{E}_{T,t}}$ is an ordinary elliptic curve over $t$, then its $p^m$-torsion is isomorphic to $\mu_{p^m,t} \times \mathbf{Z}/p^m$ and it follows that the intersection is at most $\mathbf{Z}/p$, the kernel of V. If $\widetilde{\mathcal{E}_{T,t}}$ is a supersingular elliptic curve, then its $p$-torsion subgroup is a group scheme called $\mathrm{M}_2$ (see [11](15.5)). This $\mathrm{M}_2$

cannot be embedded in a direct sum of additive groups, hence the intersection is at most the Frobenius kernel (which is isomorphic to $\alpha_{p,t}$). This completes the proof of the proposition.

# 4 Manin constants

We are now ready to apply the results of the preceding sections to the study of Manin constants. Let $\phi : X_0(p^2N) \to E$ be a strong modular parametrization, where $p > 7$ is a prime that does not divide the positive integer $N$. We suppose that $E$ has potentially good reduction at $p$, not of type $I_0^*$. Let $S$, $n$, $U$ and $T$ be as in the preceding section: $S = \mathrm{Spec}W(\overline{\mathbf{F}}_p)$, $n = \frac{p^2-1}{2}$, $U = S[\pi]$ with $\pi^n = p$ and $T = S[\pi^{\frac{n}{d}}]$, where $d$ is as in the table in proposition 4 ($T \to S$ is the minimal base change after which $E$ acquires good reduction). Let $\phi : \widetilde{X_U} \to \widetilde{\mathcal{E}_U}$ be the strong modular parametrization extended to the stable models over $U$.

Let $\omega_S$ be a Néron differential of $E$ over $S$. Then $\phi^*\omega_S$ is a meromorphic differential form on $X_0(p^2N)_S$. The valuation at $p$ of the Manin constant of $E$ is the multiplicity of the $(2,0)$-component (this is the component on which the cusp $\infty$ lies) in the divisor of $\phi^*\omega_S$. By explicit computations using minimal Weierstrass equations, it is easy to compute a Néron differential $\omega_U$ of $E$ over $U$. It turns out that $\omega_U = \pi^a\omega_S$, where $a$ is given in the following table:

| type | $II$ | $III$ | $IV$ | $IV^*$ | $III^*$ | $II^*$ |
|---|---|---|---|---|---|---|
| $a$ | $\frac{1}{6}\cdot n$ | $\frac{1}{4}\cdot n$ | $\frac{1}{3}\cdot n$ | $\frac{2}{3}\cdot n$ | $\frac{3}{4}\cdot n$ | $\frac{5}{6}\cdot n$ |

Since the parametrization $\phi$ can be extended over the stable models (see proposition 5), $\phi^*\omega_U$ is a differential form on $\widetilde{X_U}$. In particular, $\phi^*\omega_U$ is a section of the invertible sheaf of regular differentials on $\widetilde{X_{U,u}}$. We now have the following formula for the valuation $v_p(c)$ at $p$ of the Manin constant $c$ of $E$:

$$v_p(c) = \frac{1}{n}(v_C(\phi^*\omega_U) - a),$$

where $v_C(\phi^*\omega_U)$ denotes the valuation of $\phi^*\omega_U$ (as a regular differential) along the $(2,0)$-component $C$ of $\widetilde{X_{U,u}}$.

**Proposition 8** *If $\phi : \widetilde{X_{U,u}} \to \widetilde{\mathcal{E}_{U,u}}$ is separable on some component of $\widetilde{X_{U,u}}$, then $p$ does not divide $c$.*

*Sketch of proof.* According to the formula for $v_p(c)$ above, we have to show that $v_C(\phi^*\omega_U) < n + a$. By hypothesis, $\phi^*\omega_U$ gives a non-zero differential form on some component $D$ of $\widetilde{X_{U,u}}$. Let $D'$ be another component of $\widetilde{X_{U,u}}$ meeting $D$ in a point $x$. Then $v_{D'}(\phi^*\omega_U)$ can be estimated in terms of $v_x(\phi^*\omega_U|_D)$, the order of vanishing at $x$ of the restriction of $\phi^*\omega_U$ to $D$. One then proceeds in the same way with $(\pi^{-r}\phi^*\omega_U)|_{D'}$, where $r = v_{D'}(\phi^*\omega_U)$. It is clear from figure 1 that, after at most two steps, one arrives at the component $C$. It turns out that the estimates, if done properly, are sharp enough.

**Proposition 9** *Under the hypotheses of this section, one has that* $v_p(c) \leq 1$.

*Sketch of proof.* The principle is the same as in the proof of the preceding proposition, but now one has to start at a component $D$ on which $\phi$ has degree of inseparability at most 1. An easy computation shows that, in that case, $v_D(\phi^*\omega_U) \leq n$.

In order to get a stronger result, we will now consider $E$ together with $E'$, the quadratic twist of $E$ over $\mathbf{Q}(\sqrt{(\frac{-1}{p})p})$. This twist acts on the reduction types at $p$ as follows:

| original type | $II$ | $III$ | $IV$ | $IV^*$ | $III^*$ | $II^*$ |
|---|---|---|---|---|---|---|
| type of twist | $IV^*$ | $III^*$ | $III^*$ | $II$ | $III$ | $IV$ |

It is known that $E'$ is again a modular elliptic curve, and it is easy to see that the conductor of $E'$ is also $p^2N$. Let $\widetilde{E}$ be the strong curve in the isogeny class of $E'$, let $\tilde{\phi}$ be its strong modular parametrization and let $\tilde{c}$ be its Manin constant. It follows that we have a commutative diagram:

$$\begin{array}{ccc} X_0(p^2N)_{\mathbf{Q}} & \xrightarrow{\tilde{\phi}} & \widetilde{E} \\ {\scriptstyle \phi'} \searrow & & \swarrow {\scriptstyle \alpha} \\ & E' & \end{array}$$

with $\alpha$ a cyclic isogeny. Let $f\frac{dq}{q}$ and $\tilde{f}\frac{dq}{q}$ be the normalized newforms of $E$ and $\widetilde{E}$. Over $\mathbf{C}$, the modular parametrization $\phi$ is given as follows:

$$\phi : X_0(M)(\mathbf{C}) \to \mathbf{C}/\Lambda = E(\mathbf{C}) : \quad P \mapsto \int_\infty^P f\frac{dq}{q},$$

where $\Lambda$ is the period lattice of $f\frac{dq}{q}$:

$$\Lambda = \left\{ \int_\gamma f\frac{dq}{q} \ ; \ \gamma \in \mathrm{H}_1(X_0(M)(\mathbf{C}), \mathbf{Z}) \right\}.$$

This gives the following formula for $\deg(\phi)$, the degree of $\phi$:

$$\deg(\phi) = \|f\|^2/\mathrm{vol}(\mathbf{C}/\Lambda), \quad \text{where} \quad \|f\|^2 = \tfrac{i}{2}\int_{X_0(M)(\mathbf{C})} |f|^2 \frac{dq \wedge d\bar{q}}{q\bar{q}}.$$

By a standard computation, see [17], one sees that

$$\delta\Lambda \subset \widetilde{\Lambda} \subset \delta^{-1}\Lambda,$$

where $\widetilde{\Lambda}$ is the period lattice of $\tilde{f}\frac{dq}{q}$ and $\delta$ is the Gauss sum $\sqrt{(\frac{-1}{p})p}$. Since $\widetilde{\Lambda}$ is proportional to $\Lambda$, there are exactly three possibilities: $\widetilde{\Lambda} = \delta\Lambda$, $\widetilde{\Lambda} = \Lambda$ or $\widetilde{\Lambda} = \delta^{-1}\Lambda$.

In the second case, $E$ has complex multiplication. As stated in the introduction, a combination of our results and those of Stevens [14] implies that in this case $p$ does not divide $c$. Now we assume that $E$ does not have complex multiplication. The formula:

$$\|f^2\| = C \cdot [\mathrm{PSL}_2(\mathbf{Z}) : \Gamma_0(p^2N)] \cdot \mathrm{Res}_{s=2} \sum_{n=1}^{\infty} \frac{|a_n|^2}{n^s}$$

(where $C$ is some fixed constant) in [17] implies that $\|f\|^2 = \|\tilde{f}\|^2$. It now follows that $\deg(\tilde{\phi})$ equals $p^{-1}\deg(\phi)$ or $p\deg(\phi)$ in the first or third case, respectively. By comparing the stable reductions of $\phi$ and $\tilde{\phi}$, one can see that either $\phi$ or $\tilde{\phi}$ is separable on some component of $\widetilde{X_{U,u}}$. More precisely, we are in one of the two cases:

1. $\widetilde{\Lambda} = \delta\Lambda$, $\deg(\tilde{\phi}) = p^{-1}\deg(\phi)$, $\phi$ is inseparable and $\tilde{\phi}$ is separable.
2. $\widetilde{\Lambda} = \delta^{-1}\Lambda$, $\deg(\tilde{\phi}) = p\deg(\phi)$, $\phi$ is separable and $\tilde{\phi}$ is inseparable.

After replacing $E$, if necessary, by $\widetilde{E}$, we may assume that $E$ has reduction type $II$, $III$ or $IV$ at $p$. Let $\omega$ be a Néron differential of $E$ over $\mathbf{Z}$, then $\omega' = \delta^{-1}\omega$ is a Néron differential on $E'$. Let $c'$ be the Manin constant associated to $\phi'$: $\phi'^*\omega' = c'\tilde{f}\frac{dq}{q}$. Then we have the formulas:

$$\frac{\deg(\phi)}{c^2} = \frac{\|f\|^2}{\mathrm{vol}(E,\omega)} \qquad \frac{\deg(\phi')}{(c')^2} = \frac{\|\tilde{f}\|^2}{\mathrm{vol}(E',\omega')}$$

where

$$\mathrm{vol}(E,\omega) = \int_{E(\mathbf{C})} \tfrac{i}{2}\omega \wedge \overline{\omega} \quad \text{and} \quad \mathrm{vol}(E',\omega') = \int_{E'(\mathbf{C})} \tfrac{i}{2}\omega' \wedge \overline{\omega'}.$$

From these it follows directly that:

$$\deg(\tilde{\phi}) = p\deg(\phi)\frac{(c')^2}{c^2}\frac{1}{\deg(\alpha)}.$$

Since we are either in case 1 or case 2, we see that $\deg(\alpha)$ is a square. It follows from the classification of cyclic isogenies over $\mathbf{Q}$ [7] [16] that $p$ does not divide $\deg(\alpha)$. This implies that $v_p(\tilde{c}) = v_p(c')$. We arrive at:

$$v_p(\deg\tilde{\phi}) = v_p(\deg\phi) + 1 + 2v_p(\frac{\tilde{c}}{c}).$$

In case 2 above, it follows that $v_p(\tilde{c}) = v_p(c) = 0$. In case 1 above, $v_p(c) = 1$ and $v_p(\tilde{c}) = 0$. Of course, if case 1 occurs, then Manin's conjecture is false.

If $E$ has potentially supersingular reduction at $p$, then one can prove that only case 2 occurs. The reason for this is that then the $\mu_n$-action on $\widetilde{\mathcal{E}_{U,u}}$ does not commute with the Frobenius endomorphism, giving a parity condition on the degree of inseparability of $\phi$. If $E$ has potentially ordinary reduction at $p$, then these two do commute, and we cannot prove that case 1 does not occur.

# References


[1] B.J. Birch and H.P.F. Swinnerton-Dyer. *Elliptic curves and modular functions.* Modular functions of one variable IV, 2–32. Springer Lecture Notes in Mathematics 476 (1975).

[2] H. Carayol. *Sur les représentations $\ell$-adiques associées aux formes modulaires de Hilbert.* Ann. scient. Éc. Norm. Sup., série 4, t.19, 409-468 (1986).

[3] P. Deligne and M. Rapoport. *Les schémas de modules des courbes elliptiques.* Modular functions of one variable II, 143–316. Springer Lecture Notes in Mathematics 349.

[4] S.J. Edixhoven. *Minimal resolution and stable reduction of $X_0(N)$.* Preprint Utrecht November 1986, accepted for publication in the Annales de l'Institut Fourier.

[5] S.J. Edixhoven. *Stable models of modular curves and applications.* Thesis Utrecht June 1989, to be published.

[6] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies 108, Princeton University Press (1985).

[7] B. Mazur. *Rational isogenies of prime degree.* Invent. Math. 44, 129–162 (1978).

[8] B. Mazur. *Courbes elliptiques et symboles modulaires.* Séminaire Bourbaki juin 1972. Springer Lecture Notes in Mathematics 317.

[9] B. Mazur and H.P.F. Swinnerton-Dyer. *Arithmetic of Weil curves.* Invent. Math. 25, 1–16 (1974).

[10] J.-F. Mestre and J. Oesterlé. Letter to B. Gross, May 1985.

[11] F. Oort. *Commutative group schemes.* Springer Lecture Notes in Mathematics 15 (1966).

[12] M. Raynaud. *Spécialisation du foncteur de Picard.* Publications Mathématiques de l'I.H.E.S. 38 (1970).

[13] M. Raynaud. *Schémas en groupes de type (p,...,p).* Bull. Soc. Math. France 102, 241-280 (1974).

[14] G. Stevens. *Stickelberger elements and modular parametrizations of elliptic curves.* To be published.

[15] J. Tate. *Algorithm for determining the type of a singular fibre in an elliptic pencil.* In Modular Functions of One Variable IV, 33-52. Springer Lecture Notes in Mathematics 476 (1975).

[16] M. Kenku. *On the number of* $\mathbf{Q}$*-isomorphism classes of elliptic curves in each* $\mathbf{Q}$*-isogeny class.* J. of Number Theory 15, 199-202 (1982).

[17] D. Zagier. *Modular parametrizations of elliptic curves.* Canad. Math. Bull. 28(3), 372-384 (1985).

Bas Edixhoven
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720
U.S.A.