msp

Computing integral points on $X_{ns}^+(p)$

Aurélien Bajolet, Yuri Bilu and Benjamin Matschke

To the memory of Alan Baker

We develop a general method for computing integral points on modular curves, based on Baker's inequality. As an illustration, we show that for $11 \le p < 101$, the only integral points on the curve $X_{ns}^+(p)$ are the CM points.

1. Introduction

Mazur, in his celebrated work [1978] completely described the possible rational points on the modular curves $X_0(p)$, where p is a prime number. In particular, he showed that the set $X_0(p)(\mathbb{Q})$ consists only of the cusps if $p > 163$, and of the cusps and the CM-points if $37 < p \le 163$.

The curve $X_0(p)$ is associated to the Borel subgroup of $GL_2(\mathbb{F}_p)$. It is natural to ask the same question on the modular curves associated to two other important maximal subgroups of $GL_2(\mathbb{F}_p)$, the normalizers of a split Cartan or a nonsplit Cartan subgroup. See [Serre 1989, Appendix A.5] or [Baran 2010, Section 2], where all the necessary definitions are given. We shall denote these curves $X_{sp}^+(p)$ and $X_{ns}^+(p)$, respectively.[1] This problem is not only interesting by itself, but is also motivated by applications; for

---

[1]In [Serre 1989] the curves $X_{sp}^+(N)$ and $X_{ns}^+(N)$ are defined for arbitrary levels N, but in this article we restrict to prime levels only.

df^2	-3	$-3 \cdot 2^2$	$-3 \cdot 3^2$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3^1 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

df^2	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

Table 1. Rational CM j-invariants together with the discriminant of the CM order.

instance, Serre's uniformity problem about Galois representations [Bilu and Parent 2011a] would be solved if one could show that for large p the sets $X_{\mathrm{sp}}^+(p)(\mathbb{Q})$ and $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ consist only of the cusps and the CM-points (points corresponding to elliptic curves with complex multiplication). For the convenience of the reader, we reproduce the full list of the 13 rational CM j-invariants in Table 1.

Rational points on the curves $X_{\mathrm{sp}}^+(p)$ were determined in [Bilu and Parent 2011b; Bilu et al. 2013] for all $p \neq 13$; in particular, it is shown in [Bilu et al. 2013] that for $p \geq 17$ the set $X_{\mathrm{sp}}^+(p)(\mathbb{Q})$ consists only of the cusps and the CM-points. The case $p = 13$ was resolved in a recent breakthrough by Balakrishnan et al. [2019], who computed all rational points on $X_{\mathrm{sp}}^+(13)$, using Kim's "quadratic Chabauty" method.

Unfortunately, the methods of [Bilu and Parent 2011b; Bilu et al. 2013] completely fail for the curve $X_{\mathrm{ns}}^+(p)$. To the best of our knowledge, the set $X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ is not known for any prime $p \geq 17$.

More is known about *integral* points on the curves $X_{\mathrm{ns}}^+(p)$, that is, points $P \in X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ such that $j(P) \in \mathbb{Z}$, where j is the modular invariant. It is easy to see that for $p \leq 5$ this set is infinite. Kenku [1985] determined the integral points[2] on the curve $X_{\mathrm{ns}}^+(7)$; in fact, he found the 7-integral points, that is, the points $P \in X_{\mathrm{ns}}^+(p)(\mathbb{Q})$ such that the denominator of $j(P)$ is a power of 7. He used in an essential way the fact that the curve is of genus 0.

More recently, Schoof and Tzanakis [2012] determined the integral points on $X_{\mathrm{ns}}^+(11)$, using the fact that this curve is of genus 1. They showed that the only integral points on this curve are the CM-points. See also [Chen and Cummins 2004].

The methods of [Kenku 1985; Schoof and Tzanakis 2012] are quite ad hoc and do not extend to other levels.

Since the curves $X_{\mathrm{sp}}^+(13)$ and $X_{\mathrm{ns}}^+(13)$ are known to be isomorphic over $\mathbb{Q}$ (see [Baran 2014]), the already mentioned result of Balakrishnan et al. [2019] computes *rational* points on $X_{\mathrm{ns}}^+(13)$ as well. The approach of this spectacular work has some potential of extending to higher levels, but this would require substantial new ideas.

We may also mention that integral points on the curve $X_{\mathrm{ns}}^+(N)$ of certain composite levels N were determined much earlier by Heegner [1952] and Siegel [1968] in the context of the class number 1 problem; see [Serre 1989, Appendix A.5] for more details. More recently, composite levels were examined by Baran [2009; 2010]. None of these methods seems to extend to higher prime levels either.

It was observed in [Bilu 1995; 2002] that heights of integral points on a modular curve with 3 or more cusps can be effectively bounded using Baker's method; moreover, this is also true for S-integral points defined over an arbitrary number field.

---

[2] Kenku's list has two typos: instead of $j = -2^{15} 3^3 5^3 11^3$ he writes its negative; and instead of $j = 2^{15} 7^5$ he writes $j = 7^5 2^5$.

The modular curve $X_{ns}^+(p)$ has $\lceil (p-1)/2 \rceil$ cusps, so the observation above applies as soon as $p \geq 7$. Indeed, Bajolet and Sha [2014] obtained a fully explicit upper bound for the size of an integral point P on $X_{ns}^+(p)$ for an arbitrary prime $p \geq 7$. They showed that in general,

$$\log |j(P)| < 41993 \cdot 13^p \cdot p^{2p+7.5}(\log p)^2, \tag{1-1}$$

and this bound can be substantially refined if $p-1$ is divisible by a small odd prime or by 8, see Theorem 9.1 below. Sha [2013; 2014b] extended this result of Bajolet and Sha [2014] to S-integral points on rather general modular curves over arbitrary number fields, giving an explicit version of the "effective Siegel theorem for modular curves" [Bilu 2002; Bilu and Illengo 2011]. See also the recent work of Cai [2019].

Using the numerical bound (1-1), one can in principle enumerate all integral points on $X_{ns}^+(p)$. However, this bound is too huge to perform this enumeration in reasonable time.

It turns out that the huge bound can be reduced using the numerical Diophantine approximation techniques, which go back to the work of Baker and Davenport [1969]. The idea of Baker and Davenport was elaborated in [Bilu and Hanrot 1996; 1998; 1999; Bilu et al. 2001; Hanrot 2000; Pethő and Schulenberg 1987; Tzanakis and de Weger 1989] in the context of the Diophantine equations of Thue and of related types, providing practical methods for solving these equations.

In the present article we adapt these techniques to modular curves and develop an algorithm for finding integral points on the modular curve $X_{ns}^+(p)$, where $p \geq 7$ is an arbitrary prime number. Having implemented our algorithm, we prove the following.

Theorem 1.1. *Let p be a prime number, $11 \leq p \leq 97$, and let $P \in X_{ns}^+(p)(\mathbb{Q})$ be such that $j(P) \in \mathbb{Z}$. Then P is a CM point, that is, $j(P)$ is one of the 13 numbers displayed in the second line of Table 1.*

One may conjecture that for any prime $p \geq 11$ the only integral points on $X_{ns}^+(p)$ are the CM-points.

It might be useful to recall the description of integral CM-points on $X_{ns}^+(p)$. Let D be a negative quadratic discriminant with $h(D) = 1$ (that is, one of the 13 numbers in the upper row of Table 1) and let j_D be the corresponding j-invariant. Then, for $p \geq 3$, there is a point $P \in X_{ns}^+(p)(\mathbb{Z})$ with $j(P) = j_D$ if and only if $(D/p) = -1$.

As compared to the previous work, our article has two new features. The first one is using "economical" modular units made of Siegel functions. Applying explicit modular units constructed as multiplicative combinations of Siegel functions to Diophantine problems involving modular curves goes back to the work of Kubert and Lang [1975; 1981, Chapter 8]. More recently, this was successfully implemented in [Bajolet and Sha 2014; Bilu and Parent 2011a; 2011b; Sha 2014a; 2014b]. However, the units used therein, while perfect for theoretical bounds, are no longer suitable for numerical purposes. We replace them with "economical units", constructed in Sections 4–6.

Another new element, as compared to [Bilu and Hanrot 1996; 1998; 1999; Bilu et al. 2001; Hanrot 2000; Pethő and Schulenberg 1987; Tzanakis and de Weger 1989], is related to the fact that, in our case, the Baker–Davenport method alone is not sufficient to eliminate the false positives. We show that

potential integral points correspond to lattice points on a certain analytic curve. To rule them out, we cover this curve with ellipsoids and compute integral points in them using the algorithm of Fincke and Pohst [1985]. See Sections 8 and 10 for more details.

Note that our method does not use Jacobian embedding, applying thereby to curves of very high genus: for instance, the genus of $X_{\mathrm{ns}}^+(97)$ is 353. Theoretically, our method works for any prime. We did not go beyond $p = 97$ because for big p computations become too long even for modern computers. See more on this in Section 10C.

One may wonder whether our method can be adapted to a more general set up, like computing integral or even S-integral points over number fields on arbitrary modular curves with 3 or more cusps. Again, theoretically this is possible, but practical implementation may require calculations which are too hard for modern computers. A realistic task is, perhaps, computing rational points on $X_{\mathrm{ns}}^+(p)$ whose denominator is a power of p, like Kenku [1985] did for $p = 7$.

1A. ***Plan of the article.*** In Section 2 we recall basic definitions about modular curves. In particular, we review the notions of the *nearest cusp* and the *q-parameter* at a given cusp, a basic tool in the calculus on modular curves.

In Section 3 we give a general informal overview on how Baker's method applies to modular curves, highlighting both theoretical and numerical aspects.

In Sections 4 and 5 we revise the theory of modular units, an indispensable tool in the Diophantine analysis of modular curves. In Section 6 we apply this general theory in the special case of the curve $X_{\mathrm{ns}}^+(p)$, constructing especially "economical" units on this curve.

In Section 7 we evaluate the unit constructed in Section 6 at an integral point P, and express the value as a multiplicative combination of certain algebraic numbers: $U(P) = \eta_0^{b_0} \eta_1^{b_1} \cdots \eta_r^{b_r}$. We then express the exponents b_k in terms of the Galois conjugates of U and also in terms of the q-parameter of P. These expressions, while pretty trivial, will play a fundamental role in the remaining part of the article.

In Section 8 we outline the algorithm that finds all integral points based on these expressions of b_k using that all b_k are integers. The remaining sections present the different parts of the algorithm in detail.

In Section 9 we recall "Baker's bound," a huge explicit upper bound for the j-invariants of integral points P on $X_{\mathrm{ns}}^+(p)$, obtained in [Bajolet and Sha 2014] using Baker's method. This implies a very tiny lower bound for the q-parameter of P, and we show how it can be drastically improved in practical situations, using the reduction technique introduced by Baker and Davenport. This way we obtain a more reasonable lower bound for the absolute value of the q-parameter, which is still insufficient to list efficiently all integral points just by exhaustive search.

Therefore in Section 10 we present an algorithmic sieve that further reduces this set of possible values for $j(P)$ considerably. It can be seen as a much more detailed elaboration of the previous reduction step, in which some candidates for $j(P)$ may remain, and they may indeed come from integral points. In Section 10B we deal with the possible values of $j(P)$ left after the sieving. An overview of running times is given in Section 10C.

Our source code and data is available at https://github.com/bmatschke/x-nonsplit-plus/.

1B. *Notation and conventions.*

The logarithm. Unless the contrary is stated explicitly, for the complex logarithm we choose the branch satisfying

$$-\pi < \operatorname{Im}\log z \leq \pi \quad (z \in \mathbb{C}^\times).$$

Note that, with this definition, we do not always have the equality $\log(zw) = \log z + \log w$, but always have the inequality

$$|\log(zw)| \leq |\log z| + |\log w|.$$

Modular functions. Throughout the article, the letter j may have four different meanings, sometimes in the same equation, like in (2-4) and (2-8): the modular invariant $j(\tau)$ on the Poincaré plane $\mathcal{H}$; the modular invariant $j(E)$ of an elliptic curve E; the "modular invariant" rational function on a modular curve; the sum of the familiar series $j(q) = q^{-1} + 744 + 196884q + \cdots$. It should be always clear from the context which meaning of j is used. A similar convention applies to other modular functions as well.

The $O_1(\cdot)$ notation. We shall use the notation $O_1(\cdot)$, which is a quantitative analogue of the familiar $O(\cdot)$. Precisely, $A = O_1(B)$ means that $|A| \leq B$.

2. Modular curves, nearest cusps and q-parameters

Let N be a positive integer. The modular curve $X(N)$ has a geometrically irreducible model over the cyclotomic field $\mathbb{Q}(\zeta_N)$, and the Galois group $\operatorname{gal}\big(\mathbb{Q}(\zeta_N)(X(N))/\mathbb{Q}(j)\big)$ is canonically isomorphic to the quotient $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, with $\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ being the group $\operatorname{gal}\big(\mathbb{Q}(\zeta_N)(X(N))/\mathbb{Q}(\zeta_N, j)\big)$, see [Lang 1987, Chapter 6] or [Diamond and Shurman 2005, Sections 7.5 and 7.6]. We write the Galois action of $\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathbb{Q}(\zeta_N)\big(X(N)\big)$ exponentially. In the following proposition we collect the properties of this action.

Proposition 2.1. (1) *For $u \in \mathbb{Q}(\zeta_N)(X(N))$ and $\sigma \in \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})$ we have*

$$u^\sigma = u \circ \tilde{\sigma},$$

where on the right we view u as a $\Gamma(N)$-automorphic function on the extended Poincaré plane $\overline{\mathcal{H}}$, and $\tilde{\sigma}$ is a lifting of σ to $\Gamma(1) = \operatorname{SL}_2(\mathbb{Z})$. Clearly, the result is independent of the choice of the lifting.

(2) *For $\sigma \in \operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we have*

$$\zeta_N^\sigma = \zeta_N^{\det \sigma}. \tag{2-1}$$

(3) *Recall that $u \in \mathbb{Q}(\zeta_N)(X(N))$ has a "q-expansion"*

$$u = \sum_{k=k_0}^{\infty} a_k q^{k/N} \in \mathbb{Q}(\zeta_N)((q^{1/N})).$$

Then for $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ the q-expansion of u^σ is

$$u^\sigma = \sum_{k=k_0}^{\infty} a_k^\sigma q^{k/N}.$$

Proof. For item (1) see [Diamond and Shurman 2005, bottom of page 280]. Item (2) is [Diamond and Shurman 2005, Lemma 7.6.1]; see also [Lang 1987, Theorem 3 on page 66].

Item (3) is enough to verify for the functions $f_{r,s}$, as defined in [Lang 1987, Section 6.2], because they, together with j, generate the field $\mathbb{Q}(\zeta_N)(X(N))$. As explained in [Lang 1987, bottom of page 66], the q-expansion of $f_{r,s}$ is of the form

$$\sum_{k=k_0}^{\infty} a_{k,r}(\zeta_N^s)q^{k/N}, \tag{2-2}$$

where $a_{k,r}(t) \in \mathbb{Q}[t]$ are polynomials depending on k and r, but not on s.

For $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ we have $f_{r,s}^\sigma = f_{r,sd}$. Hence the q-expansion of $f_{r,s}^\sigma$ is like (2-2), but with ζ_N^s replaced by ζ_N^{sd}. Using item (2) we find

$$a_{k,r}(\zeta_N^{sd}) = a_{k,r}((\zeta_N^\sigma)^s) = a_{k,r}(\zeta_N^s)^\sigma,$$

as wanted. $\square$

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. We denote by X_G the associated modular curve. It corresponds to the G-invariant subfield of the field $\mathbb{Q}(\zeta_N)(X(N))$. The constant subfield of this field is $\mathbb{Q}(\zeta_N)^{\det G}$, where $\det : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ is the determinant, and we identify $(\mathbb{Z}/N\mathbb{Z})^\times$ with the Galois group $\mathrm{gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. In particular, if $\det G = (\mathbb{Z}/N\mathbb{Z})^\times$ then the constant subfield is $\mathbb{Q}$ and the corresponding modular curve X_G is defined (that is, has a geometrically irreducible model) over $\mathbb{Q}$.

For a subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$ put

$$G_H = \{g \in G : \det g \in H\}. \tag{2-3}$$

In particular, $G_{(\mathbb{Z}/N\mathbb{Z})^\times} = G$ and $G_1 = G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. If H is contained in $\det G$, then the subfield of $\mathbb{Q}(\zeta_N)(X(N))$ stabilized by G_H is $K(X_G)$, where $K = \mathbb{Q}(\zeta_N)^H$.

Remark 2.2. Let M_N be the subset of the abelian group $(\mathbb{Z}/N\mathbb{Z})^2$ consisting of the elements of exact order N. Then the set of cusps of the modular curve X_G is in natural one-to-one correspondence with the set $G_1 \backslash M_N$ of orbits of the natural left action of G_1 on M_N [Bilu and Illengo 2011, Lemma 2.3].

The cusps are defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$. Identifying the groups $\mathrm{gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ and $(\mathbb{Z}/N\mathbb{Z})^\times$, the natural left action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on the set $G_1 \backslash M_N$ coincides with the Galois action on the cusps. Hence, if H is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ then the set of H-orbits of cusps stands in a one-to-one correspondence with left G_H-orbits on M_N.

2A. *The nearest cusp.* Let Γ be the subgroup of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ obtained by lifting G_1. Then the set of complex points $X_G(\mathbb{C})$ is analytically isomorphic to $\Gamma \backslash \overline{\mathcal{H}}$, where $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$ is the extended Poincaré plane. Similarly, $Y_G(\mathbb{C})$ is analytically isomorphic to $\Gamma \backslash \mathcal{H}$.

We denote by $\mathcal{F}$ the familiar fundamental domain of the modular group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$: the open hyperbolic triangle with vertices $e^{i\pi/3}$, $e^{2i\pi/3}$, $i\infty$, together with the geodesics $[i, e^{i\pi/3}]$ and $[e^{i\pi/3}, i\infty)$. There is a natural bijection $Y(1)(\mathbb{C}) \leftrightarrow \mathcal{F}$, and the image of $P \in Y(1)(\mathbb{C})$ under this bijection will be denoted $\tau(P)$. More generally, the image of $P \in Y_G(\mathbb{C})$ under the map $Y_G(\mathbb{C}) \to Y(1)(\mathbb{C}) \to \mathcal{F}$ will also be denoted $\tau(P)$. Alternatively, we can define $\tau(P)$ as the single $\tau \in \mathcal{F}$ with the property

$$j(P) = j(\tau), \tag{2-4}$$

where we use the convention for j from Section 1B.

We also consider the slightly smaller set

$$\mathring{\mathcal{F}} = \{z \in \mathcal{F} : |z| > 1\}.$$

In other words, $\mathring{\mathcal{F}}$ is $\mathcal{F}$ with the geodesic $[i, e^{i\pi/3}]$ removed.

For every $\sigma \in \Gamma(1)$ we define the set $\mathcal{F}(\sigma) \subset Y_G(\mathbb{C})$ as the image of $\sigma\mathcal{F}$ in $Y_G(\mathbb{C}) = \Gamma\backslash\mathcal{H}$; similarly, $\mathring{\mathcal{F}}(\sigma)$ is the image of $\sigma\mathring{\mathcal{F}}$. Clearly

$$\mathring{\mathcal{F}}(\sigma) = \{P \in \mathcal{F}(\sigma) : |\tau(P)| > 1\}.$$

The sets $\mathcal{F}(\sigma)$ and $\mathring{\mathcal{F}}(\sigma)$ depend only on the coset $\Gamma\sigma$; in particular, there are exactly $[\Gamma(1) : \Gamma]$ distinct sets $\mathcal{F}(\sigma)$. They are pairwise disjoint and cover $Y_G(\mathbb{C})$:

$$\bigcup_{\Gamma\sigma} \mathcal{F}(\sigma) = Y_G(\mathbb{C}), \qquad \mathcal{F}(\sigma) \cap \mathcal{F}(\sigma') = \varnothing \quad (\Gamma\sigma \neq \Gamma\sigma'),$$

the union being over the cosets $\Gamma\backslash\Gamma(1)$.

Next, for every cusp c we define $\Omega_c \subseteq X_G(\mathbb{C})$ and $\mathring{\Omega}_c \subset \Omega_c$ by

$$\Omega_c = \bigcup_{\sigma(i\infty)=c} \mathcal{F}(\sigma) \cup \{c\}, \quad \mathring{\Omega}_c = \bigcup_{\sigma(i\infty)=c} \mathring{\mathcal{F}}(\sigma) \cup \{c\} = \{P \in \Omega_c : |\tau(P)| > 1\}, \tag{2-5}$$

the union being over all $\sigma \in \Gamma$ such that $\sigma(i\infty)$ represents the cusp c.

This can be made more explicit as follows. Let $e = e_c$ be the ramification index of the branch cover $X_G \to X(1)$ at c. Fix some $\sigma \in \Gamma$ such that $\sigma(i\infty)$ represents the cusp c, and define, for $k \in \mathbb{Z}$,

$$\sigma_k = \sigma \circ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}. \tag{2-6}$$

Then

$$\Omega_c = \bigcup_{k=0}^{e-1} \mathcal{F}(\sigma_k) \cup \{c\}, \quad \mathring{\Omega}_c = \bigcup_{k=0}^{e-1} \mathring{\mathcal{F}}(\sigma_k) \cup \{c\}. \tag{2-7}$$

The sets Ω_c are pairwise disjoint and cover $X_G(\mathbb{C})$:

$$\bigcup_c \Omega_c = X_G(\mathbb{C}), \qquad \Omega_c \cap \Omega_{c'} = \varnothing \quad (c \neq c').$$

If $P \in X_G(\mathbb{C})$ belongs to Ω_c, we call c the *nearest cusp* to P. Note that the set $\mathring{\Omega}_c$ is open in the complex topology, and is the maximal open subset of Ω_c.

In practical calculations, we select a full set Σ of representatives of cosets $\Gamma \backslash \Gamma(1)$. Then we have

$$X_G(\mathbb{C}) = \bigcup_{\sigma \in \Sigma} \mathcal{F}(\sigma).$$

We develop methods for finding integral points on each $\mathring{\mathcal{F}}(\sigma)$. Our methods do not work for the points P with $|\tau(P)| = 1$, but these can be found just by checking all integral values of j from 0 to 1728, see Proposition 2.3 below.

We build Σ as follows: first, for every cusp c we pick $\sigma_c \in \Gamma(1)$ such that $\sigma_c(i\infty)$ represents c. After this is done, we define Σ as the set of all $\sigma_{c,k}$ with $0 \le k \le e_c - 1$ for every c, where $\sigma_{c,k} = \sigma_c \circ \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix} \right)$. See Section 6A for a concrete example.

2B. *The q-parameter at a cusp.* For $P \in \Omega_c$ we define the q-parameter $q_c(P)$ by $q_c(P) = e^{2\pi i \tau(P)}$, with the convention $\tau(c) = i\infty$ and $q_c(c) = 0$. This q_c is a holomorphic function on $\mathring{\Omega}_c$. We have

$$j(P) = j(q_c(P)) \tag{2-8}$$

(see the same convention on j as above). Since $\operatorname{Im} \tau(P) \ge \sqrt{3}/2$ we have

$$|q_c(P)| \le e^{-\pi\sqrt{3}} < 0.0044 \quad (P \in \Omega_c). \tag{2-9}$$

As in Section 2A denote by $e = e_c$ the ramification index at c of $X_G \to X(1)$. Then q_c^{1/e_c} can be viewed as a "local analytic parameter" at c. This means the following: if $u \in \mathbb{C}(X_G)$ is a $\mathbb{C}$-rational function on X_G, then in a neighborhood of c we have

$$\log |u(P)| = \frac{\operatorname{Ord}_c u}{e_c} \log |q_c(P)| + O(1).$$

This can also be expressed in terms of Taylor expansions. Loosely speaking, it means that for $P \in \mathring{\Omega}_c$ and for a suitable choice of the e-th root $q_c(P)^{1/e}$ we have

$$u(P) = \varsigma_c q_c(P)^{\operatorname{Ord}_c u/e} + O\big(|q_c(P)|^{(\operatorname{Ord}_c u+1)/e}\big), \tag{2-10}$$

where ς_c (which is well-defined up to multiplication by an e-th root of unity) and the implied constant depend only on u, but not on P. We make this more precise as follows.

Fix $\sigma \in \Gamma(1)$ such that $\sigma(i\infty)$ represents the cusp c, and define σ_k as in (2-6). There exists a nonzero complex number $\varsigma_c = \varsigma_{c,\sigma}$ such that the following holds. For $P \in \mathring{\Omega}_c$ define $q_c(P)^{1/e} = e^{2\pi i \tau(P)/e}$. Then

$$u(P) = \varsigma_c \big(e^{2k\pi i/e} q_c(P)^{1/e}\big)^{\operatorname{Ord}_c(u)} + O\big(|q_c(P)|^{(\operatorname{Ord}_c u+1)/e}\big) \quad (P \in \mathring{\mathcal{F}}(\sigma_k), \ k \in \mathbb{Z}). \tag{2-11}$$

Due to decomposition (2-5), this gives an exact version of the "Taylor expansion" (2-10) on $\mathring{\Omega}_c$.

Note that $\varsigma_c = \varsigma_{c,\sigma}$ does depend on the choice of σ; if we change σ then ς_c would be multiplied be an e-th root of unity.

2C. *More on j*. The following property will be routinely used.

Proposition 2.3. *For a noncusp point $P \in X_G(\mathbb{C})$ the following two conditions are equivalent.*

(1) $j(P) \in \mathbb{R}$.

(2) $\mathrm{Re}(\tau(P)) \in \left\{0, \frac{1}{2}\right\}$ *or* $|\tau(P)| = 1$.

More precisely:
$$\begin{aligned}
j(P) \in [1728, +\infty) &\Leftrightarrow \mathrm{Re}(\tau(P)) = 0 \Leftrightarrow q_c(P) > 0, \\
j(P) \in (-\infty, 0] &\Leftrightarrow \mathrm{Re}(\tau(P)) = \tfrac{1}{2} \Leftrightarrow q_c(P) < 0, \\
j(P) \in [0, 1728] &\Leftrightarrow |\tau(P)| = 1,
\end{aligned}$$

where c is the nearest cusp to P.

Proof. It suffices to show that for $\tau \in \mathcal{F}$ we have

$$j(\tau) \in [1728, +\infty) \Leftrightarrow \mathrm{Re}(\tau) = 0, \tag{2-12}$$

$$j(\tau) \in (-\infty, 0] \quad \Leftrightarrow \mathrm{Re}(\tau) = \tfrac{1}{2}, \tag{2-13}$$

$$j(\tau) \in [0, 1728] \quad \Leftrightarrow |\tau| = 1. \tag{2-14}$$

Since the coefficients in the q-expansion of j are real, we have $j(iy) \in \mathbb{R}$ for $y > 0$. Using

$$j(i) = 1728, \quad \lim_{y \to +\infty} j(iy) = +\infty,$$

this proves (2-12), because j takes on $\mathcal{F}$ every complex value exactly once. In a similar fashion one proves (2-13): we have $j\left(\frac{1}{2} + iy\right) \in \mathbb{R}$ and

$$j(e^{\pi i/3}) = 0, \quad \lim_{y \to +\infty} j\left(\tfrac{1}{2} + iy\right) = -\infty.$$

Finally, using again that the coefficients in the q-expansion of j are real, we deduce that, for $\tau \in \mathcal{H}$, we have $j(-\bar{\tau}) = \overline{j(\tau)}$. Together with $j(-1/\tau) = j(\tau)$ this implies that $j(\tau) \in \mathbb{R}$ when $|\tau| = 1$. Since $j(e^{\pi i/3}) = 0$ and $j(i) = 1728$, this proves (2-14). $\square$

We shall also need an approximate formula for the j-invariant. Write the q-expansion as[3]

$$j(q) = c_{-1}q^{-1} + c_0 + c_1 q + c_2 q^2 + \cdots,$$

with $c_{-1} = 1$, $c_0 = 744$, $c_1 = 196884$, etc. For a nonnegative integer N write

$$j_N(q) = \sum_{n=-1}^{N-1} c_n q^n.$$

In particular, $j_0(q) = q^{-1}$.

---

[3]The coefficients c_n cannot be confused with the cusps.

Lemma 2.4. *For $P \in \Omega_c$ we have*

$$j(P) = j_N(q_c(P)) + R_N, \quad |R_N| \leq j(e^{-\pi\sqrt{3}}) - j_N(e^{-\pi\sqrt{3}}) \tag{2-15}$$

for any nonnegative integer N. In particular, for $N = 0$ we have

$$\left| j(P) - q_c(P)^{-1} \right| \leq 2079. \tag{2-16}$$

Proof. Since j is $\Gamma(1)$-invariant, we may assume that c is the cusp at infinity and $q_c(P) = q(P)$. Since the coefficients c_n are known to be positive and $|q(P)| \leq e^{-\pi\sqrt{3}}$, we have

$$\left| j(P) - j_N(q_c(P)) \right| \leq \sum_{n=N}^{\infty} c_n |q(P)|^n \leq \sum_{n=N}^{\infty} c_n |e^{-\pi\sqrt{3}}|^n = j(e^{-\pi\sqrt{3}}) - j_N(e^{-\pi\sqrt{3}}),$$

proving (2-15). In particular, for $N = 0$ we obtain

$$\left| j(P) - q_c(P)^{-1} \right| \leq j(e^{-\pi\sqrt{3}}) - e^{\pi\sqrt{3}} < 2309.6 - 230.7 < 2079. \qquad \square$$

Note that the exact value of $j(e^{-\pi\sqrt{3}})$ is available: $j(e^{-\pi\sqrt{3}}) = 40500(35010 - 20213\sqrt{3})$.

3. Integral points and Baker's method on modular curves

In this section we give a general overview of Baker's method applied to modular curves. For more details, see [Bajolet and Sha 2014; Bilu 2002] and Sha's thesis [2013].

Let N and G be as in Section 2, let K be a number field containing $\mathbb{Q}(\zeta_N)^{\det G}$ and $\mathcal{O}_K$ the ring of integers of K. We define the set of integral points

$$X_G(\mathcal{O}_K) = \{ P \in X_G(K) : j(P) \in \mathcal{O}_K \}.$$

Recall that the *height* of $\alpha \in \mathcal{O}_K$ is defined by

$$h(\alpha) = [K : \mathbb{Q}]^{-1} \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log^+ |\alpha^\sigma|, \quad \log^+ = \max\{\log, 0\}.$$

the sum being over the complex embeddings of K.

We want to bound the height $h(j(P))$ for $P \in X_G(\mathcal{O}_K)$. We show how to do this under the assumption

$$\nu_\infty(G) \geq 3, \tag{3-1}$$

where $\nu_\infty(G)$ denotes the number of cusps of X_G.

A *modular unit* is a rational function (defined over $\overline{K}$) on X_G with no zeros and no poles outside the cusps. Equivalently, $u \in \overline{K}(X_G)$ is a modular unit if both u and u^{-1} are integral over the ring $\mathbb{Q}[j]$. Principal divisors of modular units form a subgroup in the group of degree 0 divisors supported on the cusps. The latter is a free abelian group of rank $\nu_\infty(G) - 1$, so the group of principal divisors of modular units must be of rank not exceeding $\nu_\infty(G) - 1$. It is of fundamental importance for us that it is of the maximal possible rank; this is sometimes called the *Manin–Drinfeld theorem*.

Theorem 3.1. *The principal divisors of modular units form a free abelian group of rank $v_\infty(G) - 1$.*

See [Lang 1995, Chapter 4, Theorem 2.1]. Here is an immediate consequence.

Corollary 3.2. *Assume that $v_\infty(G) \geq 3$. Then for any cusp c there exists a nonconstant modular unit u such that $u(c) = 1$.*

If $j(P) \in \mathcal{O}_K$ then $\mathrm{h}(j(P)) = [K : \mathbb{Q}]^{-1} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log^+ |j(P)^\sigma|$, the sum being over the complex embeddings of K. For some embedding σ we have $\mathrm{h}(j(P)) \leq \log |j(P)^\sigma|$. We fix this embedding from now on and view K as a subfield of $\mathbb{C}$. Thus, we have to bound $|j(P)|$ from above.

The point P belongs to one of the sets Ω_c, defined in (2-5), and the corresponding c is the "nearest cusp" to P. Now, since $v_\infty(G) \geq 3$, we may use Corollary 3.2 and find a nonconstant modular unit u with $u(c) = 1$. The rational function u is defined over the number field $K(\zeta_N)$.

If $u(P) = 1$ then it is easy to bound P as one of the zeros of the rational function $u - 1$. From now on we assume that $u(P) \neq 1$. Since $u(c) = 1$, we have

$$u(P) = 1 + O(|q_c(P)|^{1/e_c}).$$

(Here and below in this section, the constant implied by the $O(\cdot)$-notation, as well as by the Vinogradov notation "$\ll$" and "$\gg$," may depend on N and K, but not on P.) Thus, $u(P)$ is a complex algebraic number, distinct from 1 but "close" to 1 if $q_c(P)$ is small.

Since both u and u^{-1} are integral over $\mathbb{Q}[j]$, there exist nonzero $A_1, A_2 \in \mathbb{Z}$, which can be easily determined explicitly, such that $A_1 u$ and $A_2 u^{-1}$ are integral over $\mathbb{Z}[j]$. Since $j(P) \in \mathcal{O}_K$, both $A_1 u(P)$ and $A_2 u(P)^{-1}$ belong to $\mathcal{O}_{K(\zeta_N)}$. It follows that there are only finitely many possibilities for the principal ideal $(u(P))$ (viewed as a fractional ideal in the field $K(\zeta_N)$).

Fixing a system $\eta_1, \ldots, \eta_r$ of fundamental units of $K(\zeta_N)$, we obtain $u(P) = \eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r}$, where η_0 belongs to a finite subset of K (that can be explicitly determined), and $b_1, \ldots, b_r$ are rational integers depending on P. We obtain the inequality

$$\left| \eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r} - 1 \right| \ll q_c(P)^{1/e_c}. \tag{3-2}$$

Let $B = \max(|b_1|, \ldots, |b_r|)$. It is easy to show that $B \ll \mathrm{h}(\eta)$, see [Bilu 2002, bottom of page 77]. It follows that $B \ll \mathrm{h}(u(P)) + 1$. On the other hand, the general property of quasiequivalence of heights on an algebraic curve implies that $\mathrm{h}(u(P)) \ll \mathrm{h}(j(P)) + 1$. It follows that

$$B \ll \mathrm{h}(j(P)) \leq \log |j(P)| = \log |q_c(P)^{-1}| + O(1). \tag{3-3}$$

On the other hand, one can bound the left-hand side of (3-2) from below using the so-called *Baker's inequality*, which implies that either the left-hand side of (3-2) is 0 (in which case $u(P) = 1$ and $\mathrm{h}(j(P))$ is bounded), or it is bounded from below by $\exp(-\kappa \log \max(B, 3))$, where κ is a positive effective constant depending on $\eta_0, \eta_1, \ldots, \eta_r$ but independent of B. Combining this with (3-2), we obtain the estimate $\log |q_c(P)^{-1}| \ll \log \max(B, 3)$. Together with (3-3) this bounds $|q_c(P)|$ away from zero, which

implies a bound for $|j(P)|$ from above. See [Bajolet and Sha 2014], where this approach is used to bound explicitly integral points on $X_{\mathrm{ns}}^+(p)$ for $p \geq 7$.

In a similar fashion one can study S-integral points on X_G: the new ingredients to be added are the p-adic version of Baker's inequality, due to Yu [2007], and the p-adic analogue of the notion of the "nearest cusp," see [Bilu and Parent 2011a, Section 3]. We do not go into this in the present article.

To make the argument above explicit, one needs to construct modular units explicitly. The standard tool for this is *Siegel functions*, see Section 4 below. One also needs explicit version for various statements above like the quasiequivalence of heights, etc. All this can be found in the Ph.D. thesis of Sha [2013; 2014b].

In the present work, we are interested in a somewhat different task: not just to bound the heights of integral points, but to determine them completely. We restrict ourselves to the case $K = \mathbb{Q}$ and $N = p$ a prime number. In this case the most interesting class of modular curves for which integral points are unknown is $X_{\mathrm{ns}}^+(p)$, when the group G is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

The principal point here is that bounding the height of integral points, even explicitly in all parameters, is not sufficient for the actual calculation of the points. The problem is that the bounds obtained by Baker's method are excessively huge and not suitable for direct enumeration.

Fortunately, one can reduce Baker's bound using the technique of numerical Diophantine approximation introduced by Baker and Davenport [1969]. This reduction is described in detail in [Bilu and Hanrot 1996; 1999; Hanrot 2000] in the context of the Diophantine equation of Thue. Recall that this is the equation of the form $f(x, y) = A$, where the $f(x, y) \in \mathbb{Z}[x, y]$ is a $\mathbb{Q}$-irreducible form of degree $n \geq 3$, and A is a nonzero integer. In [Bilu and Hanrot 1998] the method was extended to the superelliptic Diophantine equations. Here we adapt this reduction method to modular curves.

Several observations are to be made.

(1) Usually, to perform the computations, one should know explicitly the algebraic data of the number field(s) involved (in the case of Thue equation, this is the field generated over $\mathbb{Q}$ by a root of $f(1, y)$). By the algebraic data we mean here the unit group (with explicit generators), the class group (again, for every class one should have an explicit ideal representing this class), and so on. Fortunately, in the special case of the curve $X_{\mathrm{ns}}^+(p)$ these tasks are radically simplified.

First, the field we are going to deal with is the real cyclotomic field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ (or a subfield, see below) for which the unit group (or at least a full-rank subgroup of the latter, which is sufficient, see below) is given explicitly by the *circular units*. To be precise, the index of the group of circular units in the full unit group of $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ is equal to the real class number h_p^+; see, for instance, [Washington 1982, Theorem 8.2].

In the range $p < 100$ that we are working, we have $h_p^+ = 1$, see the recent article of Miller [2015], who extended the earlier work of Masley [1978]. Hence in this range circular units form the full unit group.

Second, the only ideal we are going to deal with is the one above p, which is principal and has an obvious explicit generator $(\zeta_p - \bar{\zeta}_p)^2$. This was already used in [Bilu et al. 2001] for solving Thue equations $\Phi_n(x, y) = p$, where $\Phi_n(1, y)$ is the n-th real cyclotomic polynomial, and p is a prime divisor of n.

(2) To make the calculations more efficient, it is in some cases useful to replace the field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ by a smaller subfield, if possible. This was suggested in [Bilu and Hanrot 1999] and was very efficiently exploited in [Bilu et al. 2001].

In the setting of the present paper, with this trick we reduced the running for $p = 97$ by a factor of 4.5 using the subfield of degree 16. We also tried to use the degree 12 subfield, however then the sieves become too imprecise so that it becomes more expensive to exclude potential lattice points on the curve γ (cf. Section 10), and we ended up with a running time improvement by only a factor of 1.5.

(3) In principle, it is not necessary to have the full unit group; a full-rank subgroup would suffice, as explained in [Hanrot 2000]. In particular, since circular units form a full rank subgroup for all p, our method must work for all primes, not only for those where the circular units form the full unit group. Note that this was used already in [Bilu et al. 2001] (in a different context).

In the present work we use only full unit groups as they were always computable for our parameters, either due to the above-mentioned result of Miller [2015], or using the [PARI/GP 2017] package. However, one should keep this opportunity in mind for further applications.

(4) Adapting numerical methods developed for Thue equations to modular curves is not straightforward. In the Thue case one has formulas with very strong error estimates, typically $O(|x|^{-n})$, where n is the degree of the equation; see, for instance [Bilu and Hanrot 1996, Proposition 2.4.1]. This is quite good even for small solutions x.

However, for modular curves of level p we have, typically, errors $O(|j(P)|^{-1/p})$. Larger errors mean that we have to check more false candidates to find all solutions. Therefore in Section 10 we considerably improve the involved sieves. If the error bounds are too weak, one can use higher order asymptotic expansions for the modular functions involved, see the Appendix. At the point where this becomes computationally too expensive, we stop the sieve and start an extra search, which checks all j with small modulus separately.

4. Siegel functions

In this section we recall the principal facts about Klein forms and Siegel functions. For more details the reader can consult [Kubert and Lang 1981, Section 2.1; Koo and Shin 2010]. We call a positive integer N a *denominator* of $a \in \mathbb{Q}$ if $Na \in \mathbb{Z}$. For instance, 2020 is a denominator of $\frac{1}{2}$.

4A. *Klein forms and Siegel functions.* Let $\tilde{a} = (\tilde{a}_1, \tilde{a}_2) \in \mathbb{Q}^2$ be such that $\tilde{a} \notin \mathbb{Z}^2$. We denote by $\mathfrak{k}_{\tilde{a}}(\tau)$ the Klein form associated to $\tilde{a}$, which is a holomorphic function on the Poincaré plane $\mathcal{H}$. We collect some properties of Klein forms in the proposition below.

Proposition 4.1. (1) *The Klein forms do not vanish on $\mathcal{H}$.*

(2) *The Klein forms behave well under the action of $\Gamma(1)$: for $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Gamma(1)$ we have*

$$\mathfrak{k}_{\tilde{a}} \circ \sigma(\tau) = (c\tau + d)^{-1} \mathfrak{k}_{\tilde{a}\sigma}(\tau),$$

where $\sigma(\tau) = \dfrac{a\tau+b}{c\tau+d}$. *In particular, with* $\sigma = -I$ *this gives*

$$\mathfrak{k}_{-\tilde{\boldsymbol{a}}} = -\mathfrak{k}_{\tilde{\boldsymbol{a}}}. \tag{4-1}$$

(3) *For* $\tilde{\boldsymbol{a}} = (\tilde{a}_1, \tilde{a}_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ *and* $\tilde{\boldsymbol{b}} = (\tilde{b}_1, \tilde{b}_2) \in \mathbb{Z}^2$ *we have*

$$\mathfrak{k}_{\tilde{\boldsymbol{a}}+\tilde{\boldsymbol{b}}} = \varepsilon(\tilde{\boldsymbol{a}}, \tilde{\boldsymbol{b}})\mathfrak{k}_{\tilde{\boldsymbol{a}}}, \quad \varepsilon(\tilde{\boldsymbol{a}}, \tilde{\boldsymbol{b}}) = (-1)^{\tilde{b}_1\tilde{b}_2+\tilde{b}_1+\tilde{b}_2}e^{\pi i(\tilde{a}_1\tilde{b}_2-\tilde{a}_2\tilde{b}_1)}.$$

Notice that $\varepsilon(\tilde{\boldsymbol{a}}, \tilde{\boldsymbol{b}})^{2N} = 1$, *where* N *is a denominator of* $\tilde{\boldsymbol{a}}$ *(a common denominator of* $\tilde{a}_1$ *and* $\tilde{a}_2$*).*

(4) *Let* N *be a denominator of* $\tilde{\boldsymbol{a}}$. *Then* $\mathfrak{k}_{\tilde{\boldsymbol{a}}}$ *is "nearly"* $\Gamma(N)$-*automorphic of weight* -1. *Precisely, for* $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$ *we have*

$$\mathfrak{k}_{\tilde{\boldsymbol{a}}} \circ \sigma(\tau) = \varepsilon'(\tilde{\boldsymbol{a}}, \sigma)(c\tau+d)^{-1}\mathfrak{k}_{\tilde{\boldsymbol{a}}}(\tau), \quad \varepsilon'(\tilde{\boldsymbol{a}}, \sigma)^{2N} = 1.$$

The following result is a consequence of the properties above.

Proposition 4.2. *Let* N *be a denominator of* $\tilde{\boldsymbol{a}}$. *Then* $\mathfrak{k}_{\tilde{\boldsymbol{a}}}^{2N}$ *depends only on the residue class of* $\tilde{\boldsymbol{a}}$ *modulo* $\mathbb{Z}^2$, *and it is* $\Gamma(N)$-*automorphic of weight* $-2N$.

Further, for $\tilde{\boldsymbol{a}} = (\tilde{a}_1, \tilde{a}_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Siegel function* $g_{\tilde{\boldsymbol{a}}}(\tau)$ by

$$g_{\tilde{\boldsymbol{a}}}(\tau) = \mathfrak{k}_{\tilde{\boldsymbol{a}}}(\tau)\eta(\tau)^2,$$

where $\eta(\tau)$ is the Dedekind η-function.

Since $\eta(\tau)^{24} = \Delta(\tau)$ is $\Gamma(1)$-automorphic of weight 12, Proposition 4.2 implies the following.

Theorem 4.3. *In the set-up of Proposition 4.2, the function* $g_{\tilde{\boldsymbol{a}}}^{12N}$ *depends only on the residue class of* $\tilde{\boldsymbol{a}}$ *modulo* $\mathbb{Z}^2$, *and is* $\Gamma(N)$-*automorphic of weight* 0.

It follows, in particular, that Siegel functions $g_{\tilde{\boldsymbol{a}}}$ are algebraic over the field $\mathbb{C}(j)$ (because so are $\Gamma(N)$-automorphic functions). In addition to this, $g_{\tilde{\boldsymbol{a}}}$ is holomorphic and does not vanish on the Poincaré plane $\mathcal{H}$ (because so are the Klein forms and the Dedekind η). It follows that both $g_{\tilde{\boldsymbol{a}}}$ and $g_{\tilde{\boldsymbol{a}}}^{-1}$ must be integral over the ring $\mathbb{C}[j]$. Actually, a stronger assertion holds (see, for instance, Proposition 2.2 from [Bilu and Parent 2011b]).

Proposition 4.4. *Let* N *be the smallest denominator of* $\tilde{\boldsymbol{a}}$ *and* ζ_N *a primitive* N-*th root of unity. Then both* $g_{\tilde{\boldsymbol{a}}}$ *and* $(1 - \zeta_N)g_{\tilde{\boldsymbol{a}}}^{-1}$ *are integral over* $\mathbb{Z}[j]$.

4B. *An approximate formula.* As usual, write $q = q(\tau) = e^{2\pi i\tau}$. For a rational number a we define $q^a = e^{2\pi ia\tau}$. Then the Siegel function $g_{\tilde{\boldsymbol{a}}}$ has the following infinite product presentation [Kubert and Lang 1981, page 29]:

$$g_{\tilde{\boldsymbol{a}}}(\tau) = -q^{B_2(\tilde{a}_1)/2}e^{\pi i\tilde{a}_2(\tilde{a}_1-1)}\prod_{n=0}^{\infty}(1 - q^{n+\tilde{a}_1}e^{2\pi i\tilde{a}_2})(1 - q^{n+1-\tilde{a}_1}e^{-2\pi i\tilde{a}_2}), \tag{4-2}$$

where $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial. Together with Proposition 4.1(3), this implies that

$$\operatorname{Ord}_q g_{\tilde{\boldsymbol{a}}} = \ell_{\tilde{\boldsymbol{a}}} := B_2(\tilde{a}_1 - \lfloor\tilde{a}_1\rfloor)/2. \tag{4-3}$$

Here the q-order Ord_q is defined by $\lim_{q \to 0} q^{\mathrm{Ord}_q\, g_{\tilde{a}}}\, g_{\tilde{a}}(q) \neq 0, \infty$.

In fact, we have the following quantitative statement.

Proposition 4.5. *Put*

$$\varrho_{\tilde{a}} = \begin{cases} -e^{\pi i \tilde{a}_2(\tilde{a}_1 - 1)}, & \tilde{a}_1 \neq 0, \\ -e^{\pi i \tilde{a}_2(\tilde{a}_1 - 1)}(1 - e^{2\pi i \tilde{a}_2}), & \tilde{a}_1 = 0. \end{cases} \tag{4-4}$$

Then, for a nonzero $\tilde{a} = (\tilde{a}_1, \tilde{a}_2) \in \mathbb{Q}^2 \cap [0, 1)^2$ and $\tau \in \mathcal{H}$ we have

$$\left| \log \frac{g_{\tilde{a}}(\tau)}{\varrho_{\tilde{a}} q^{\ell_{\tilde{a}}}} \right| \leq \begin{cases} \dfrac{1}{1 - |q|} \left(\dfrac{|q|^{\tilde{a}_1}}{1 - |q|^{\tilde{a}_1}} + \dfrac{|q|^{1 - \tilde{a}_1}}{1 - |q|^{1 - \tilde{a}_1}} \right), & \tilde{a}_1 > 0, \\ \dfrac{2|q|}{(1 - |q|)^2}, & \tilde{a}_1 = 0. \end{cases} \tag{4-5}$$

Proof. For $|z| < 1$ we have $\left| \log(1 + z) \right| \leq |z|/(1 - |z|)$. Hence, when $\tilde{a}_1 > 0$, we can bound the terms of the product expansion (4-2) as

$$\left| \log(1 - q^{n + \tilde{a}_1} e^{2\pi i \tilde{a}_2}) \right| \leq \frac{|q|^{n + \tilde{a}_1}}{1 - |q|^{\tilde{a}_1}}, \quad \left| \log(1 - q^{n + 1 - \tilde{a}_1} e^{-2\pi i \tilde{a}_2}) \right| \leq \frac{|q|^{n + 1 - \tilde{a}_1}}{1 - |q|^{1 - \tilde{a}_1}}.$$

Adding this up for all $n \geq 0$, we obtain

$$\left| \log \frac{g_{\tilde{a}}(\tau)}{\varrho_{\tilde{a}} q^{\ell_{\tilde{a}}}} \right| \leq \sum_{n=0}^{\infty} \left(\frac{|q|^{n + \tilde{a}_1}}{1 - |q|^{\tilde{a}_1}} + \frac{|q|^{n + 1 - \tilde{a}_1}}{1 - |q|^{1 - \tilde{a}_1}} \right) = \frac{1}{1 - |q|} \left(\frac{|q|^{\tilde{a}_1}}{1 - |q|^{\tilde{a}_1}} + \frac{|q|^{1 - \tilde{a}_1}}{1 - |q|^{1 - \tilde{a}_1}} \right),$$

which proves (4-5) in the case $\tilde{a}_1 > 0$.

In the case $\tilde{a}_1 = 0$ we rewrite (4-2) as

$$g_{\tilde{a}}(\tau) = \varrho_{\tilde{a}} q^{\ell_{\tilde{a}}} \prod_{n=1}^{\infty} (1 - q^n e^{2\pi i \tilde{a}_2})(1 - q^n e^{-2\pi i \tilde{a}_2}).$$

We bound

$$\left| \log(1 - q^n e^{2\pi i \tilde{a}_2}) \right|, \left| \log(1 - q^n e^{-2\pi i \tilde{a}_2}) \right| \leq \frac{|q|^n}{1 - |q|} \quad (n \geq 1).$$

Adding this up for $n \geq 1$, we prove (4-5) in the case $\tilde{a}_1 = 0$ as well. $\square$

Corollary 4.6. *In the set-up of Proposition 4.5 assume that $\tau \in \mathcal{F}$. Let N be a denominator of $\tilde{a}_1$, and assume that $N \geq 5$. Then*

$$\left| \log \frac{g_{\tilde{a}}(\tau)}{\varrho_{\tilde{a}} q^{\ell_{\tilde{a}}}} \right| \leq N |q|^{1/N}. \tag{4-6}$$

Proof. Assume first that $\tilde{a}_1 > 0$, in which case $\tilde{a}_1, 1 - \tilde{a}_1 \geq 1/N$. The function

$$x \mapsto \frac{x}{1 - x} + \frac{|q| x^{-1}}{1 - |q| x^{-1}}$$

is increasing on the interval $[|q|^{1/2}, 1)$. Hence

$$\frac{|q|^{\tilde{a}_1}}{1 - |q|^{\tilde{a}_1}} + \frac{|q|^{1 - \tilde{a}_1}}{1 - |q|^{1 - \tilde{a}_1}} \leq \frac{|q|^{1/N}}{1 - |q|^{1/N}} + \frac{|q|^{1 - 1/N}}{1 - |q|^{1 - 1/N}}$$

Since $\tau \in \mathcal{F}$, we have $|q| \geq e^{-\pi\sqrt{3}}$. Using the assumption $N \geq 5$, we obtain

$$\frac{|q|^{1/N}}{1 - |q|^{1/N}} \leq \frac{|q|^{1/N}}{1 - e^{-\pi\sqrt{3}/N}} = \frac{e^{\pi\sqrt{3}/N}}{e^{\pi\sqrt{3}/N} - 1}|q|^{1/N} \leq e^{\pi\sqrt{3}/5}\frac{N}{\pi\sqrt{3}}|q|^{1/N},$$

$$\frac{|q|^{1-1/N}}{1 - |q|^{1-1/N}} \leq \frac{|q|^{3/5}}{1 - |q|^{4/5}}|q|^{1/N} \leq \frac{e^{-3\pi\sqrt{3}/5}}{1 - e^{-4\pi\sqrt{3}/5}}|q|^{1/N} \leq \frac{N}{5}\frac{e^{-3\pi\sqrt{3}/5}}{1 - e^{-3\pi\sqrt{3}/5}}|q|^{1/N}.$$

It follows that

$$\left|\log \frac{g_{\tilde{a}}(\tau)}{\varrho_{\tilde{a}}q^{\ell_{\tilde{a}}}}\right| \leq \frac{1}{1 - e^{-\pi\sqrt{3}}}\left(\frac{e^{\pi\sqrt{3}/5}}{\pi\sqrt{3}} + \frac{e^{-3\pi\sqrt{3}/5}}{5(1 - e^{-4\pi\sqrt{3}/5})}\right)N|q|^{1/N} < 0.56N|q|^{1/N},$$

which proves (4-6), in a stronger form, in the case $\tilde{a}_1 > 0$.

The case $\tilde{a}_1 = 0$ is much simpler:

$$\left|\log \frac{g_{\tilde{a}}(\tau)}{\varrho_{\tilde{a}}q^{\ell_{\tilde{a}}}}\right| \leq \frac{2|q|}{(1 - |q|)^2} \leq \frac{2e^{-4\pi\sqrt{3}/5}}{(1 - e^{-\pi\sqrt{3}})^2}|q|^{1/N} \leq 0.03|q|^{1/N},$$

which is much better than (4-6).   □

More refined approximate formulas can be found in the Appendix, see Proposition A.1 therein.

4C. *Simplest modular units.* Now let us fix a positive integer N. We have the natural group isomorphism $(N^{-1}\mathbb{Z}/\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2$, and, with some abuse of speech, we identify the two groups. In particular, for $\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ we have the corresponding element in $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$, and for this latter we may fix a lifting $\tilde{\boldsymbol{a}} \in N^{-1}\mathbb{Z}^2$, which will be called a lifting of $\boldsymbol{a}$ to $N^{-1}\mathbb{Z}^2$.

By Theorem 4.3, for $\boldsymbol{a} \in N^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ the function

$$u_{\boldsymbol{a}} := g_{\tilde{\boldsymbol{a}}}^{12N}$$

does not depend on a particular choice of the lifting $\tilde{\boldsymbol{a}}$ and defines a $\mathbb{C}$-rational function on the modular curve $X(N)$. Identity (4-1) implies that $u_{\boldsymbol{a}} = u_{-\boldsymbol{a}}$.

The infinite product (4-2) implies that the q-expansion of $u_{\boldsymbol{a}}$ has coefficients in the cyclotomic field $\mathbb{Q}(\zeta_N)$. By [Shimura 1971, Proposition 6.9(1)], it follows that $u_{\boldsymbol{a}} \in \mathbb{Q}(\zeta_N)(X(N))$. Moreover, the Galois action of the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathbb{Q}(\zeta_N)(X(N))$ (see Section 2) coincides with the action induced by the natural right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the set $(\mathbb{Z}/N\mathbb{Z})^2$ in the following sense: for a nonzero $\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ and $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we have

$$u_{\boldsymbol{a}\sigma} = u_{\boldsymbol{a}}^{\sigma}. \tag{4-7}$$

See [Bilu and Parent 2011a, Section 4.2] for more details.

The functions $u_{\boldsymbol{a}}$ give the simplest explicit examples of the *modular units*, already mentioned in Section 3: they have no zeros and no poles outside the cusps. It follows that their principal divisors generate a free abelian subgroup of rank at most $v_\infty(N) - 1$, where $v_\infty(N)$ is the number of cusps of $X(N)$. It turns out that this rank is the maximal possible, which provides an explicit form of the Manin–Drinfeld theorem (Theorem 3.1):

Theorem 4.7. *The principal divisors (u_a) generate a free abelian group of rank $v_\infty(N) - 1$.*

For the proof see Theorem 3.1 in [Kubert and Lang 1981, Chapter 2].

In fact, one can show that already the principal divisors (u_a), where a runs through the set M_N, consisting of the elements of $(\mathbb{Z}/N\mathbb{Z})^2$ of exact order N, generate a free abelian group of rank $v_\infty(N) - 1$. The number of such a is $2v_\infty(N)$. It follows that, besides the relations $u_a = u_{-a}$, there can exist exactly one relation between the principal divisors (u_a) with $a \in M_N$. This relation is

$$\sum_{a \in M_N} (u_a) = 0.$$

In fact, we have a more precise statement.

Lemma 4.8. *In the above set-up we have*

$$\prod_{a \in M_N} u_a = \pm \Phi_N(1)^{12N}, \tag{4-8}$$

where $\Phi_N(t)$ is the N-th cyclotomic polynomial. In particular, if $N = p$ is a prime number, we have

$$\prod_{a \in M_p} u_a = \pm p^{12p}. \tag{4-9}$$

This will be used in the proof of the principal relation (Section 7) that our algorithm is based upon.

Proof. Since the set M_N is stable with respect to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the left-hand side of (4-8) is stable with respect to the Galois action over the field $\mathbb{Q}(X(1))$. Hence it is a unit on the curve $X(1)$, defined over $\mathbb{Q}$. Since $X(1)$ has only one cusp, it has no nonconstant units. Hence the left-hand side of (4-8) is a constant belonging to $\mathbb{Q}$.

To determine the value of this constant, we evaluate it at the cusp at infinity. For each $a \in (\mathbb{Z}/N\mathbb{Z})$ we choose the lifting $\tilde{a} = (\tilde{a}_1, \tilde{a}_2) \in \mathbb{Q}^2$ such that $0 \le a_1, a_2 < 1$. The left-hand side of (4-8) is a product of a root of unity and the terms of the type $(1 - e^{2\pi i a_2} q^{n+\tilde{a}_1})^{12N}$ and of the type $(1 - e^{2\pi i - a_2} q^{n+1-\tilde{a}_1})^{12N}$, where n runs through nonnegative integers, and $(\tilde{a}_1, \tilde{a}_2)$ runs through the liftings of the elements of the set M_N. When we set $q = 0$, all these terms become 1 except the terms $(1 - e^{2\pi i a_2} q^{n+a_1})^{12N}$ with $n = 0$ and $a_1 = 0$. Hence, up to a root of unity, the left-hand side of (4-8) is

$$\prod_{\substack{a_2 \in N^{-1}\mathbb{Z}/\mathbb{Z} \\ a_2 \text{ is of order } N}} (1 - e^{2\pi i a_2})^{12N} = \prod_{\substack{0 \le k < N \\ (k,N)=1}} (1 - e^{2\pi i k/N})^{12N} = \Phi_N(1)^{12N}.$$

Since the only roots of unity in $\mathbb{Q}$ are ± 1, this proves (4-8) and the lemma. $\qquad\square$

5. General modular units

In this section we review and complement some of the results of Kubert and Lang [1981]. Our purpose is to construct "economical" modular units on the curve X_G.

The "naive" approach is as follows. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and H a subgroup of $\det G$, which itself is a subgroup in $(\mathbb{Z}/N\mathbb{Z})^\times$, viewed as the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_N)$. Then H left-acts naturally on the set of the cusps of X_G. Denote by $\nu_\infty(G)$ the number of cusps and by $\nu_\infty(G, H)$ the number of H-orbits of cusps.

On the other hand, the group G_H, defined in (2-3), right-acts on the set $(\mathbb{Z}/N\mathbb{Z})^2$. If $\mathcal{O} \subset (\mathbb{Z}/N\mathbb{Z})^2$ is a nonzero orbit of this action, then

$$\prod_{\boldsymbol{a} \in \mathcal{O}} u_{\boldsymbol{a}} \tag{5-1}$$

is a rational function on the curve X_G defined over the field $\mathbb{Q}(\zeta_N)^H$.

It is not difficult to deduce from Theorem 4.7 that the principal divisors defined by products (5-1), where $\mathcal{O}$ runs the nonzero G_H-orbits, generate a free abelian group whose rank is $\nu_\infty(G, H) - 1$.

Product (5-1) can be written as

$$\prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}}^{12N}, \tag{5-2}$$

where $\tilde{\boldsymbol{a}} \in N^{-1}\mathbb{Z}^2$ is a lifting of $\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2$, as defined in Section 4C. The principal goal of this section is constructing rational functions on X_G of the form

$$\prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}}^{m}, $$

where m is much smaller than $12N$, which is crucial for numerical purposes.

5A. *Quadratic relations.* Let N be a positive integer. As in Section 4C, we identify the groups $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$ and $(\mathbb{Z}/N\mathbb{Z})^2$, which allows us to lift every $\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ to some $\tilde{\boldsymbol{a}} \in N^{-1}\mathbb{Z}^2$. By a lifting of a set $A \subset (\mathbb{Z}/N\mathbb{Z})^2$ we mean a mapping $A \to N^{-1}\mathbb{Z}^2$ such that for every $\boldsymbol{a} \in A$ its image $\tilde{\boldsymbol{a}} \in N^{-1}\mathbb{Z}^2$ is a lifting of $\boldsymbol{a}$ in the sense defined above.

Our principal tool will be the following result:

Theorem 5.1 (see [Kubert and Lang 1981, Theorem 5.2 in Chapter 3]). *To every nonzero $\boldsymbol{a} = (a_1, a_2) \in (\mathbb{Z}/N\mathbb{Z})^2$ we associate an integer $m(\boldsymbol{a})$. Fix a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of the set of nonzero elements of $(\mathbb{Z}/N\mathbb{Z})^2$. Put*

$$\Lambda = \sum_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} m(\boldsymbol{a}). \tag{5-3}$$

(1) *Assume that N is odd. Then*

$$\prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} \mathfrak{k}_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})} \tag{5-4}$$

is $\Gamma(N)$-automorphic (of weight $-\Lambda$) if and only if

$$\sum_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} m(\boldsymbol{a})a_1^2 = \sum_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} m(\boldsymbol{a})a_2^2 = \sum_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} m(\boldsymbol{a})a_1 a_2 = 0. \tag{5-5}$$

(2) *Assume that* $\gcd(N, 6) = 1$. *Then the function*

$$\prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})} \tag{5-6}$$

is $\Gamma(N)$-*automorphic* (*of weight* 0) *if and only if* (5-5) *holds and* $12 \mid \Lambda$.

Remark 5.2. (1) Kubert and Lang call (5-5) "quadratic relations" (modulo N).

(2) One may note that

$$\prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})} = \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} \mathfrak{k}_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})} \cdot \Delta^{\Lambda/12}, \tag{5-7}$$

where $\Delta = \eta^{24}$.

(3) The assumption $\gcd(N, 6) = 1$ is purely technical: in a slightly modified form the statement holds true when N is divisible by 2 and/or by 3. However, assuming that $\gcd(N, 6) = 1$ will not hurt us, since we shall apply Theorem 5.1 only when N is prime and $N \geq 7$.

(4) Theorem 5.1 implies that product (5-6) defines a function $u \in \mathbb{C}(X(N))$. By considering the q-expansion, as in Section 4C, we conclude that in fact $u \in \mathbb{Q}(\zeta_N)(X(N))$.

Contrary to product (5-2), product (5-6) may depend on the choice of the lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$. Proposition 4.1(3) implies that if we choose a different lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}'$ then (5-4) and (5-6) will be multiplied by a $2N$-th root of unity. Though this is pretty trivial, we state this as a proposition for further reference.

Proposition 5.3. *For every nonzero* $\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ *pick an integer* $m(\boldsymbol{a})$ *and fix* **two** *liftings* $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ *and* $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}'$ *of the set of nonzero elements of* $(\mathbb{Z}/N\mathbb{Z})^2$. *Then there exists a* $2N$-*th root of unity* ε *such that*

$$\prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} \mathfrak{k}_{\tilde{\boldsymbol{a}}'}^{m(\boldsymbol{a})} = \varepsilon \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} \mathfrak{k}_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})}. \tag{5-8}$$

If additionally $12 \mid \Lambda$, *with* Λ *defined in* (5-3), *then*

$$\prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}'}^{m(\boldsymbol{a})} = \varepsilon \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})}. \tag{5-9}$$

If $2 \mid m(\boldsymbol{a})$ *for every* $\boldsymbol{a}$ *then*

$$\varepsilon^N = 1. \tag{5-10}$$

Proof. Statements (5-8) and (5-10) follow from Proposition 4.1(3), and (5-9) follows from (5-8) and (5-7).

$\square$

5B. *Galois action.* As we mentioned in Section 4C, the Galois action by the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the "simplest" modular units $u_{\boldsymbol{a}} = g_{\tilde{\boldsymbol{a}}}^{12N}$ is very easy to describe: it is given by relation (4-7). We want to obtain a similar result for "general" modular units (5-6).

Proposition 5.4. *Assume the set-up of Theorem 5.1(2), so that*

$$u = \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}}^{m(\boldsymbol{a})}$$

defines a function in $\mathbb{Q}(\zeta_N)(X_G)$ (see Remark 5.2(4)).

(1) Assume that $\sigma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and let $\tilde{\sigma}$ be a lifting of σ to $\Gamma(1)$. Then

$$u^{\sigma} = \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}\tilde{\sigma}}^{m(\boldsymbol{a})}. \tag{5-11}$$

(2) Assume that $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then it has a lifting $\tilde{\sigma} \in \mathrm{M}_2(\mathbb{Z})$ such that (5-11) holds.

Proof. The first part is a consequence of Propositions 2.1(1) and 4.1(2) and Equation (5-7). Indeed, write $\tilde{\sigma} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and recall that $\Delta = \eta^{24}$ is $\Gamma(1)$-automorphic of weight 12. We obtain

$$
\begin{aligned}
u^{\sigma}(\tau) &= u \circ \tilde{\sigma}(\tau) \\
&= \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} (\mathfrak{k}_{\tilde{\boldsymbol{a}}} \circ \tilde{\sigma}(\tau))^{m(\boldsymbol{a})} \cdot (\Delta \circ \tilde{\sigma}(\tau))^{\Lambda/12} \\
&= (c\tau + d)^{-\Lambda} \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} \mathfrak{k}_{\tilde{\boldsymbol{a}}\tilde{\sigma}}(\tau)^{m(\boldsymbol{a})} \cdot (c\tau + d)^{\Lambda} \Delta(\tau)^{\Lambda/12} \\
&= \prod_{\substack{\boldsymbol{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \boldsymbol{a} \neq 0}} g_{\tilde{\boldsymbol{a}}\tilde{\sigma}}(\tau)^{m(\boldsymbol{a})},
\end{aligned}
$$

as wanted.

In the proof of the second part, we may assume that σ is of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, because any $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ can be presented as $\sigma_1 \sigma_2$ with $\sigma_1 \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and σ_2 of this form. We lift $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ as $\tilde{\sigma} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \tilde{d} \end{smallmatrix}\right)$, and the result follows immediately from Proposition 2.1(3) and the infinite product (4-2). $\qquad \square$

5C. *Economical modular units on X_G.* In this section to avoid technicalities we restrict to prime level. Thus, let $p \geq 5$ be a prime number, G a subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$ and H a subgroup in $\det G$. The group G_H, defined in (2-3), right-acts on the set $M_p = \mathbb{F}_p^2 \setminus \{0\}$ (as in the previous section, we tacitly identify the sets $\mathbb{F}_p^2$ and $(p^{-1}\mathbb{Z}/\mathbb{Z})^2$). Let $\mathcal{O} \subset M_p$ be an orbit of this action, or, more generally, a G_H-invariant subset of M_p. We fix a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of the set M_p (as defined in the beginning of Section 5A) and we want to find an exponent m such that

$$u = \prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}}^{m} \tag{5-12}$$

defines a function in $K(X_G)$, where $K = \mathbb{Q}(\zeta_p)^H$. Clearly, $m = 12p$ would do. It turns out that in some cases one can do much better, sometimes introducing a root of unity factor. We fix a p-th primitive root of unity and denote it by ζ_p.

Theorem 5.5. *Let $p \geq 5$ be a prime number and $G \ni -I$ a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that $|G|$ is not divisible by p. Let H be a subgroup of $\det G$ and $\mathcal{O} \subset M_p$ a G_H-invariant subset of M_p satisfying*

$$\sum_{\boldsymbol{a} \in \mathcal{O}} a_1^2 = \sum_{\boldsymbol{a} \in \mathcal{O}} a_1 a_2 = \sum_{\boldsymbol{a} \in \mathcal{O}} a_2^2 = 0. \tag{5-13}$$

Let m be an integer such that

$$2 \mid m, \quad 12 \mid m|\mathcal{O}|. \tag{5-14}$$

Fix a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of the set $\mathcal{O}$ and define u as in (5-12). Then u defines a function in $\mathbb{Q}(\zeta_p)(X_G)$ (denoted by u as well). Further, there exists $k \in \mathbb{Z}$ (which is unique $\mod p$ when $H \neq 1$) such that $\zeta_p^k u \in K(X_G)$, where $K = \mathbb{Q}(\zeta_p)^H$.

The proof requires a lemma, which is the simplest special case of the Kummer theory (see any textbook in algebra).

Lemma 5.6. *Let p be a prime number and F a field of characteristic distinct from p. Let α be an element in the algebraic closure $\bar{F}$, and $\zeta_p \in \bar{F}$ a primitive p-th root of unity. Assume that $\alpha^p \in F$. Then either $[F(\alpha) : F] = p$ or there exists $k \in \mathbb{Z}$ (which is unique $\mod p$ when $\zeta_p \notin F$) such that $\zeta_p^k \alpha \in F$. In particular, if $\zeta_p \in F$ then either $[F(\alpha) : F] = p$ or $\alpha \in F$.*

Proof of Theorem 5.5. Theorem 5.1 together with Remark 5.2(4) imply that u defines a function in $\mathbb{Q}(\zeta_p)(X(p))$. We want to study the Galois action of G_H on u. Thus, fix $\sigma \in G_H$. Proposition 5.4(2) implies that there exists a lifting $\tilde{\sigma} \in M_2(\mathbb{Z})$ such that

$$u^\sigma = \prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}\tilde{\sigma}}^m. \tag{5-15}$$

Since $\mathcal{O}$ is G_H-invariant, we have $\mathcal{O}\sigma^{-1} = \mathcal{O}$. Consider a different lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}'$ of $\mathcal{O}$ defined by $\tilde{\boldsymbol{a}}' = \widetilde{\boldsymbol{a}\sigma^{-1}}\tilde{\sigma}$, where $\widetilde{\boldsymbol{a}\sigma^{-1}}$ is the lifting of $\boldsymbol{a}\sigma^{-1}$. Then (5-15) can be rewritten as

$$u^\sigma = \prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}'}^m.$$

Now Proposition 5.3 implies that u^σ/u is a p-th root of unity. We have proved that u^p is invariant under the Galois action by G_H, which implies that $u^p \in K(X_G)$, the G_H-invariant subfield of $\mathbb{Q}(\zeta_p)(X(p))$. Since the degree $\left[\mathbb{Q}(\zeta_p)(X(p)) : K(X_G)\right] = |G_H|$ is not divisible by p (because $|G|$ is not divisible by p by the assumption), Lemma 5.6 completes the proof. $\square$

There is an important special case when u itself belongs to $K(X_G)$, without multiplication by a root of unity. Assume that G_H contains $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. In this case $\boldsymbol{a} = (a_1, a_2)$ belongs to a G_H-orbit $\mathcal{O}$ if and only if its "complex conjugate" $\bar{\boldsymbol{a}} = (a_1, -a_2)$ does. We say that a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ *respects complex conjugation*

if the following holds: if $\boldsymbol{a} = (a_1, a_2) \in \mathcal{O}$ is lifted to $\tilde{\boldsymbol{a}} = (\tilde{a}_1, \tilde{a}_2)$, then the lifting of $\bar{\boldsymbol{a}}$ is $(\tilde{a}_1, -\tilde{a}_2)$. This can be expressed briefly as $\tilde{\bar{\boldsymbol{a}}} = \bar{\tilde{\boldsymbol{a}}}$.

Corollary 5.7. *In the set-up of Theorem 5.5 assume that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in G_H$ and that the lifting respects complex conjugation. Then $u \in K(X_G)$.*

Proof. The assumption $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in G_H$ implies that $K \subseteq \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. Further, since the lifting respects complex conjugation, we have $u^\iota = u$, where $\iota = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The subfield of $\mathbb{Q}(\zeta_p)(X_G)$ stabilized by ι is $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)(X_G)$. Thus, $u \in \mathbb{Q}(\zeta_p + \bar{\zeta}_p)(X_G)$ and $\zeta_p^k u \in K(X_G)$ with $K \subseteq \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. It follows that ζ_p^k lies in $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ which is only possible if $\zeta_p^k = 1$. $\qquad\square$

5D. *An approximate formula.* Using Proposition 4.5 and Corollary 4.6, we may obtain approximate expressions for the modular units constructed in Section 5C. Let p, G, H and $\mathcal{O}$ be as in Section 5C. In particular, as in Theorem 5.5, we will assume that

$$|G| \text{ is not divisible by } p.$$

Let c be a cusp of X_G. We define the sets Ω_c, $\overset{\circ}{\Omega}_c$ and the q-parameter q_c as in Sections 2A and 2B, that is, $q_c(P) = e^{2\pi i \tau(P)}$ for $P \in \Omega_c$. We also fix $\sigma \in \Gamma(1)$ such that $\sigma(i\infty)$ represents the cusp c and define σ_k as in (2-6).

Since the ramification of $X(p) \to X(1)$ at all cusps is p, the ramification of $X_G \to X(1)$ at c is either 1 or p. Moreover, since $|G|$ is not divisible by p, the ramification is p at all cusps.

As in the previous section, we fix a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of the set M_p.

For a subset $A \in M_p$ define the quantities

$$\ell_A = \sum_{\boldsymbol{a} \in A} \ell_{\tilde{\boldsymbol{a}}}, \quad \varrho_A = \prod_{\boldsymbol{a} \in A} \varrho_{\tilde{\boldsymbol{a}}}, \tag{5-16}$$

where $\ell_{\tilde{\boldsymbol{a}}}$ is defined in (4-3) and $\varrho_{\tilde{\boldsymbol{a}}}$ is defined in (4-4). Note that ℓ_A is independent of the fixed lifting, but ϱ_A depends on it and is well-defined only up to multiplication by a p-th root of unity. However, we will mainly deal with the absolute value $|\varrho_A|$, which is independent of the lifting.

Proposition 5.8. *Assume that G is a semisimple subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and that $\mathcal{O}$ and m satisfy the hypothesis of Theorem 5.5. Define u as in (5-12), and define $\varsigma_c = \varsigma_{c,\sigma}$ as in Section 2B. Then*

$$\frac{\mathrm{Ord}_c u}{p} = m\ell_{\mathcal{O}\sigma}, \quad \varsigma_c = \varrho_{\mathcal{O}\sigma}^m \cdot (a \ p\text{-th root of unity}). \tag{5-17}$$

Furthermore, for $P \in \mathcal{F}(\sigma_k)$ we have

$$\log|u(P)| = m\ell_{\mathcal{O}\sigma} \log|q_c(P)| + m\log|\varrho_{\mathcal{O}\sigma}| + O_1\big(pm|\mathcal{O}||q_c(P)|^{1/p}\big). \tag{5-18}$$

Proof. Replacing G by $\sigma^{-1}G\sigma$ and $\mathcal{O}$ by $\mathcal{O}\sigma$, we may assume that c is represented by $i\infty$. We may further assume, without loss of generality, that $\sigma = I$. In this special case Proposition 5.8 follows immediately from Proposition 4.5 and Corollary 4.6 applied with $N = p$ to every $\tilde{\boldsymbol{a}}$ lifting some $\boldsymbol{a} \in \mathcal{O}$; recall that $p \geq 5$ by the assumption. $\qquad\square$

In the sieving algorithm of Section 10 we use more refined approximate formulas from the Appendix.

5E. *An example.* We conclude this section with an example. It will not be used in the sequel, but it gives a good illustration of how Theorem 5.5 can be used.

We take as G the diagonal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and set $H = \{1, -1\}$, so that

$$G_H = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix} \right) : ad = \pm 1 \right\}$$

and $K = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$.

The right G_H-action on M_p has $(p-1)/2$ distinct orbits. They are of the form $\{ \boldsymbol{a} : a_1 a_2 = \pm c \}$ with $c = 1, \ldots, (p-1)/2$. The quadratic relations (5-13) are clearly satisfied, and to have (5-14) it suffices to take

$$m = \begin{cases} 2, & p \equiv 1 \bmod 3, \\ 6, & p \equiv -1 \bmod 3. \end{cases}$$

Selecting a lifting respecting the complex conjugation, we obtain $(p-1)/2$ modular units in the field $K(X_G)$.

6. Cusp points and units on $X_{\mathrm{ns}}^+(p)$

From now on we restrict to the case when $N = p$ is a prime number and G is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. A very detailed account of various properties of this curve (even for an arbitrary N) can be found in Sections 3 and 6 of Baran's article [2010].

We may and will assume that

$$G = \left\{ \begin{pmatrix} \alpha & \Xi\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \Xi\beta \\ -\beta & -\alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p, \ (\alpha, \beta) \neq (0,0) \right\}, \tag{6-1}$$

where Ξ is a quadratic nonresidue modulo p, which will be fixed from now on. In particular, one can take $\Xi = -1$ if $p \equiv 3 \bmod 4$.

We fix until the end of the article a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of the set M_p to $p^{-1}\mathbb{Z}^2$, which respects complex conjugation (as defined before Corollary 5.7) and which has in addition to this the following property:

$$\text{If } \tilde{\boldsymbol{a}} = (\tilde{a}_1, \tilde{a}_2) \text{ is a lifting of } \boldsymbol{a} \in M_p, \text{ then } 0 \leq \tilde{a}_1 < 1. \tag{6-2}$$

6A. *Cusps.* The curve $X_G = X_{\mathrm{ns}}^+(p)$ has $(p-1)/2$ cusps, defined over the real cyclotomic fields $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$, and the Galois group $\mathrm{gal}\big(\mathbb{Q}(\zeta_p + \bar{\zeta}_p)/\mathbb{Q}\big) = \mathbb{F}_p^\times / \{\pm 1\}$ acts transitively on the cusps.

According to Remark 2.2, the cusps stay in one-to-one correspondence with the orbits of the left G_1-action on the set $M_p = \mathbb{F}_p^2 \setminus \{(0,0)\}$. These orbits are the sets defined by $x^2 - \Xi y^2 = \pm c$, where c runs through representatives of cosets $\mathbb{F}_p^\times / \{\pm 1\}$, the cusp at infinity corresponding to $c = 1$.

For every $c \in \mathbb{F}_p^\times / \{\pm 1\}$ fix $(a, b) \in \mathbb{F}_p^2$ such that $a^2 - \Xi b^2 = c^{-1}$ and let σ_c be a lifting of the matrix $\left(\begin{smallmatrix} ca & b\Xi \\ cb & a \end{smallmatrix} \right)$ to $\Gamma(1)$. For $c = 1$ we take $(a, b) = (1, 0)$ and $\sigma_1 = I$. Then the set $\left\{ \sigma_c(i\infty) : c \in \mathbb{F}_p^\times / \{\pm 1\} \right\}$ is a

full system of representatives of cusps on $\overline{\mathcal{H}}$, and the set

$$\Sigma = \left\{ \sigma_c \circ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_p^\times / \{\pm 1\}, \ k = 0, \ldots, p-1 \right\}$$

is a complete system of representatives of cosets of $\Gamma_{\mathrm{ns}}^+ \backslash \Gamma(1)$. This is a special case of the construction explained in Section 2A.

In the sequel we fix a subgroup H of $\mathbb{F}_p^\times$ containing -1 and put $d = [\mathbb{F}_p^\times : H]$. In particular,

$$d = [K : \mathbb{Q}],$$

where $K = \mathbb{Q}(\zeta_p)^H$. The group H acts on the set of cusps by Galois conjugation, and this action has exactly d orbits, each of them being defined over K as a set. The Galois group $\mathrm{gal}(K/\mathbb{Q}) = \mathbb{F}_p^\times / H$ acts on the set of H-orbits transitively. These H-orbits of cusps are in one-to-one correspondence with the sets defined by $x^2 - \Xi y^2 \in cH$, with cH running through the cosets $\mathbb{F}_p^\times / H$.

6B. *Units*. Besides the left action, the group G_H acts on the set M_p from the right. There are again d orbits of this action, and they are defined by $\Xi x^2 - y^2 \in cH$. These orbits will be used to define modular units in $K(X_G)$. Recall that we fixed a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of M_p to $p^{-1}\mathbb{Z}^2$, respecting the complex conjugation.

Theorem 6.1. *Let $\mathcal{O}$ be a right G_H-orbit on M_p. Pick a lifting $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ of $\mathcal{O}$ to $p^{-1}\mathbb{Z}^2$. Put*

$$m = \begin{cases} 2, & \text{if } 3 \mid (p+1)|H|, \\ 6, & \text{otherwise.} \end{cases} \tag{6-3}$$

Then the product

$$u_{\mathcal{O}} = \prod_{\boldsymbol{a} \in \mathcal{O}} g_{\tilde{\boldsymbol{a}}}^m \tag{6-4}$$

is well-defined (it depends only on the orbit $\mathcal{O}$ but not on the particular lifting) and it defines a function in $K(X_G)$.

We deduce this theorem from Theorem 5.5 (more precisely from Corollary 5.7) using some elementary lemmas about finite fields. We thank Ioulia Baoulina for useful explanations and for the proof of Lemma 6.3 below.

Lemma 6.2. *Let $P(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial over a finite field $\mathbb{F} = \mathbb{F}_q$ of degree bounded by $\deg P < n(q-1)$. Then $\sum_{\boldsymbol{b} \in \mathbb{F}^n} P(\boldsymbol{b}) = 0$.*

Proof. This is Lemma 6.4 in [Lidl and Niederreiter 1997]. □

Lemma 6.3. *Let $\mathbb{F}$ be a finite field of odd characteristic and having more than 3 elements. Further, let $f(x, y), g(x, y) \in \mathbb{F}[x, y]$ be quadratic forms over $\mathbb{F}$. Then for $c \in \mathbb{F}^\times$ we have*

$$\sum_{\substack{a,b \in \mathbb{F} \\ g(a,b) = \pm c}} f(a, b) = 0,$$

where the sum is over the pairs $(a, b) \in \mathbb{F}^2$ such that $g(a, b) = \pm c$.

Proof. Write $q = |\mathbb{F}|$, so that $\mathbb{F} = \mathbb{F}_q$. Then

$$\sum_{\substack{a,b \in \mathbb{F} \\ g(a,b)=\pm c}} f(a,b) = \sum_{a,b \in \mathbb{F}} f(a,b)\big(2 - (g(a,b)-c)^{q-1} - (g(a,b)+c)^{q-1}\big).$$

We have

$$f(x,y)\big(2 - (g(x,y)-c)^{q-1} - (g(x,y)+c)^{q-1}\big) = -2f(x,y)g(x,y)^{q-1} + \big[\text{terms of degree} < 2(q-1)\big],$$

and Lemma 6.2 implies that the sum from the assertion is equal to $-2\sum_{a,b \in \mathbb{F}} f(x,y)g(x,y)^{q-1}$. The latter sum is $\sum_{a,b \in \mathbb{F}, \, g(a,b) \neq 0} f(a,b)$, which again by Lemma 6.2 and by the assumption $q > 3$ is equal to $-\sum_{a,b \in \mathbb{F}, \, g(a,b)=0} f(a,b)$. If the quadratic form $g(x,y)$ is anisotropic over $\mathbb{F}$ then the latter sum consists only of the term $f(0,0)$ and there is nothing to prove. And if it is isotropic then after a change of variables we may assume that $g(x,y) = xy$. Writing $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$, the latter sum becomes $(\alpha + \gamma)\sum_{a \in \mathbb{F}} a^2$. Lemma 6.2 implies that $\sum_{a \in \mathbb{F}} a^2 = 0$ when $\mathbb{F}$ has more than 3 elements. This completes the proof. $\qquad\square$

Proof of Theorem 6.1. Recall that the orbit $\mathcal{O}$ consists of $(x,y) \in \mathbb{F}_p^2$ satisfying $\Xi x^2 - y^2 \in cH$ with some $c \in \mathbb{F}_p^\times$. Since $H \ni -1$, Lemma 6.3 implies that the quadratic relations (5-13) hold true. Further, for each $c \in \mathbb{F}_p^\times$ there is exactly $p+1$ elements of $\mathbb{F}_{p^2}$ of norm c, which implies that our orbit $\mathcal{O}$ has exactly $(p+1)|H|$ elements, and with our choice of m the divisibility conditions (5-14) hold true as well. Corollary 5.7 now implies that $u \in K(X_G)$.

Finally, $u_{\mathcal{O}}$ does not depend on the lifting. Indeed, if we choose two different liftings respecting complex conjugation and obtain the products, say, u and u', then u/u' is a p-th root of unity by Proposition 5.3. On the other hand, $u, u' \in K(X_G)$, which implies that $u/u' \in K$, a totally real field. Hence $u = u'$. The theorem is proved. $\qquad\square$

6C. *Galois action on the units.* Consider first the case of general algebraic curves. The proof of the following proposition is a standard exercise in Galois theory.

Proposition 6.4. *Let K/k be a finite Galois extension of fields of characteristic 0, and let X be a projective curve defined (that is, having a geometrically irreducible model) over k. Then the extension $K(X)/k(X)$ is Galois and the restriction map*

$$\text{gal}\big(K(X)/k(X)\big) \to \text{gal}(K/k), \quad \sigma \mapsto \sigma|_K$$

defines isomorphism of Galois groups. Further, for $P \in X(k)$ and $u \in K(X)$ we have $u(P) \in K$, and given $\sigma \in \text{gal}\big(K(X)/k(X)\big) = \text{gal}(K/k)$ we have $u^\sigma(P) = u(P)^\sigma$.

In our case the group

$$\text{gal}\big(K(X_G)/\mathbb{Q}(X_G)\big) = \text{gal}(K/\mathbb{Q}) = G/G_H = \mathbb{F}_p^\times/H$$

acts transitively and faithfully on the right G_H-orbits, and this action agrees with the Galois action: for $\sigma \in \mathrm{gal}(K/\mathbb{Q}) = \mathbb{F}_p^\times/H$ we have $u_{\mathcal{O}}^\sigma = u_{\mathcal{O}\sigma}$. Fixing an orbit $\mathcal{O}$ and putting $U = u_{\mathcal{O}}$, we obtain the following.

Proposition 6.5. *For $P \in X_G(\mathbb{Q})$ we have $U(P) \in K$ and $U^\sigma(P) = U(P)^\sigma$ for $\sigma \in \mathrm{gal}(K/\mathbb{Q})$.*

Since distinct orbits are disjoint, Theorem 4.7 and the discussion thereafter have the following consequence (recall that $d = [K : \mathbb{Q}] = [\mathbb{F}_p^\times : H]$).

Proposition 6.6. *The d principal divisors (U^σ), $\sigma \in \mathrm{gal}(K/\mathbb{Q})$, generate an abelian group of rank $d-1$, the only relation being $\sum_\sigma (U^\sigma) = 0$. In particular, if $d \geq 3$ and $\sigma \neq 1$ then U and U^σ are multiplicatively independent modulo the constants.*

Finally, Equation (4-9) implies that

$$\prod_{\sigma \in \mathrm{gal}(K/\mathbb{Q})} U^\sigma = \pm p^m. \tag{6-5}$$

Indeed, arguing as in the proof of Lemma 4.8, we show that the left-hand side of (6-5) is a rational constant. It also follows from our definitions that the left-hand side of (6-5) is equal to

$$\prod_{\boldsymbol{a} \in M_P} g_{\tilde{\boldsymbol{a}}}^m.$$

Razing this to $(12p/m)$-th power, we obtain the left-hand side of (4-9). This proves (6-5).

7. The principal relation

We retain the set-up of Section 6 and in particular that of Section 6C:

- $p \geq 5$ is a prime number, ζ_p is a primitive p-th root of unity.
- $\boldsymbol{a} \mapsto \tilde{\boldsymbol{a}}$ is a lifting of the set $M_p = \mathbb{F}_p^2 \setminus \{(0, 0)\}$ which respects complex conjugation and satisfies (6-2).
- G is the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, realized as in (6-1).
- H is a subgroup of $\mathbb{F}_p^\times$, $H \ni -1$.
- $m = 2$ or 6 according to (6-3).
- $K = \mathbb{Q}(\zeta_p)^H$ and $d = [K : \mathbb{Q}] = [\mathbb{F}_p^\times : H]$.
- $\mathcal{O}$ is a fixed right G_H-orbit in M_p and $U = u_{\mathcal{O}}$ as defined in Theorem 6.1. It might be worth pointing out that

$$|H| = \frac{p-1}{d}, \quad |\mathcal{O}| = (p+1)|H| = \frac{p^2-1}{d}. \tag{7-1}$$

We fix a system $\eta_1, \ldots, \eta_{d-1}$ of fundamental units of the totally real field K. We also put

$$\eta_0 = \mathcal{N}_{\mathbb{Q}(\zeta_p)/K}(1 - \zeta_p). \tag{7-2}$$

Clearly, η_0 generates the prime ideal $\mathfrak{p}$ of K above p; recall that $\mathfrak{p}^d = (p)$.

Recall that we call a point $P \in X_G(\mathbb{Q})$ *integral* if $j(P) \in \mathbb{Z}$. Proposition 4.4 implies that for an integral point P on X_G, the principal ideal $(U(P))$ is an integral ideal of the field K, and moreover it is a power of $\mathfrak{p}$. Since $\mathfrak{p}^\phi = \mathfrak{p}$ for $\phi \in \mathrm{gal}(K/\mathbb{Q})$, relation (6-5) implies that $(U(P)) = \mathfrak{p}^m$. Thus, we have

$$U(P) = \pm\eta_0^{b_0}\eta_1^{b_1}\cdots\eta_{d-1}^{b_{d-1}}, \tag{7-3}$$

where $b_0 = m$ and $b_1, \ldots, b_{d-1}$ are some rational integers depending on P.

The purpose of this section is to express the exponents b_k in terms of the point P; more precisely, in terms of $q_c(P)$, where c is the nearest cusp to P (Section 2A). This can be viewed as an analogue of Equation (20) on page 378 of [Bilu and Hanrot 1996].

For $\phi \in \mathrm{gal}(K/\mathbb{Q})$ we have[4]

$$U^\phi(P) = \pm(\eta_0^\phi)^{b_0}(\eta_1^\phi)^{b_1}\cdots(\eta_{d_1}^\phi)^{b_{d-1}}.$$

Fix an ordering on the elements of the Galois group: $\mathrm{gal}(K/\mathbb{Q}) = \{\phi_0 = \mathrm{id}, \phi_1, \ldots, \phi_{d-1}\}$. Since the real algebraic numbers $\eta_0, \eta_1, \ldots, \eta_{d-1}$ are multiplicatively independent, the $d \times d$ real matrix $(\log|\eta_\ell^{\phi_k}|)_{0 \le k, \ell \le d-1}$ is nonsingular. Let $(\alpha_{k\ell})_{0 \le k, \ell \le d-1}$ be the inverse matrix. Then

$$b_k = \sum_{\ell=0}^{d-1} \alpha_{k\ell} \log|U^{\phi_\ell}(P)| \quad (k = 0, 1, \ldots, d-1). \tag{7-4}$$

We will call (7-4) the *principal relation*: It will play crucial role in our reduction and enumeration algorithms.

Combining (7-4) with Proposition 5.8, we may express b_k in terms of $q_c(P)$. Let us introduce some notation. Let c be a cusp of X_G. Define the following quantities:

$$\delta_{c,k} = -m\sum_{\ell=0}^{d-1}\alpha_{k\ell}\ell_{\mathcal{O}\phi_\ell\sigma}, \qquad \vartheta_{c,k} = m\sum_{\ell=0}^{d-1}\alpha_{k\ell}\log|\varrho_{\mathcal{O}\phi_\ell\sigma}| \quad (k = 0, 1, \ldots, d-1),$$

$$\kappa = \max_k \sum_{\ell=0}^{d-1}|\alpha_{k\ell}|, \qquad \Theta = \kappa mp(p^2-1)d^{-1}, \tag{7-5}$$

where ℓ_A and ϱ_A are defined in (5-16), and σ is an element in $\Gamma(1)$ such that $\sigma(i\infty)$ represents c. It follows from (5-17) that $\delta_{c,k}$ and $\vartheta_{c,k}$ are independent of the choice of σ.

Remark 7.1. It is easy to see that $\delta_{c,0} = 0$ and at least one of the numbers $\delta_{c,1}, \delta_{c,2}, \ldots, \delta_{c,d-1}$ is nonzero. Indeed, we have

$$\begin{pmatrix} \mathrm{Ord}_c\, U^{\phi_0} \\ \mathrm{Ord}_c\, U^{\phi_1} \\ \vdots \\ \mathrm{Ord}_c\, U^{\phi_{d-1}} \end{pmatrix} = (\log|\eta_\ell^{\phi_k}|)_{0 \le k, \ell \le d-1} \begin{pmatrix} \delta_{c,0} \\ \delta_{c,1} \\ \vdots \\ \delta_{c,d-1} \end{pmatrix}. \tag{7-6}$$

---

[4]In the sequel we use the letter ϕ rather than σ to denote elements of $\mathrm{gal}(K/\mathbb{Q})$.

Multiplying both sides by the row vector $(1, \ldots, 1)$ on the left, we obtain $\delta_{c,0} = 0$. Further, since the column vector on the left of (7-6) is nonzero, so is the column vector on the right.

Proposition 7.2. *Let P be an integral point on X_G and c its nearest cusp (that is, $P \in \Omega_c$). Then for $k = 0, \ldots, d-1$ we have*

$$b_k = \delta_{c,k} \log |q_c(P)|^{-1} + \vartheta_{c,k} + O_1\big(\Theta |q_c(P)|^{1/p}\big). \tag{7-7}$$

In particular,

$$|b_k| \leq |\delta_{c,k}| \log |q_c(P)|^{-1} + |\vartheta_{c,k}| + \Theta. \tag{7-8}$$

Proof. Using (5-18) and (7-1), we obtain

$$\log |U(P)| = m\ell_{\mathcal{O}\sigma} \log |q_c(P)| + m \log |\varrho_{\mathcal{O}\sigma}| + O_1\big(mp(p^2 - 1)d^{-1}|q_c(P)|^{1/p}\big),$$

and the same holds true when U is replaced by U^ϕ and $\mathcal{O}$ by $\mathcal{O}\phi$ for any $\phi \in \mathrm{gal}(K/\mathbb{Q})$. Now the result follows by (7-4) and (7-5). $\qquad\square$

8. Outline of the algorithm

In order to compute the integral points on $X_{\mathrm{ns}}^+(p)$, we need to consider them on each $\mathcal{F}(\sigma)$ (see Section 2A), $\sigma \in \Sigma$, where Σ is the full system of representatives of cosets $\Gamma\backslash\Gamma(1)$ as given in Section 6A. Let us fix one such σ until the end of Section 10, and we denote by c the cusp represented by $\sigma(i\infty)$, so that $\mathcal{F}(\sigma) \subset \Omega_c$.

The principal relation (7-4) can be written as

$$b = A \cdot \lambda, \tag{8-1}$$

where $b = (b_k)_{0 \leq k \leq d-1}$, $A = (\alpha_{k\ell})_{0 \leq k, \ell \leq d-1}$, and $\lambda = (\log |U^{\phi_\ell}(P)|)_{0 \leq \ell \leq d-1}$.

For integral points P with $j(P) \notin \{1, 2, \ldots, 1727\}$ with closest cusp c, the associated q_c-parameter is real and nonzero, and more precisely

$$q_c(P) \in I_0 := [-e^{-\pi\sqrt{3}}, e^{-2\pi}] \setminus \{0\}.$$

Suppose further that P lies in $\mathcal{F}(\sigma)$, where we use the notation from Section 2A. The points in $\mathcal{F}(\sigma)$ with real q_c-parameter are in bijective correspondence with I_0 via the map q_c. Restricting λ to those points of interest within $\mathcal{F}(\sigma)$, we obtain a curve in $\mathbb{R}^d$ parametrized over I_0, and we denote it $\lambda_\sigma(q_c) : I_0 \to \mathbb{R}^d$ with "variable" $q_c \in I_0$.

Furthermore let us define a curve $\gamma_\sigma := A \cdot \lambda_\sigma$ in $\mathbb{R}^d$, which is equally parametrized by q_c over the same domain I_0, and which depends as well on the chosen $\sigma \in \Sigma$. Recall that the matrix A depends only on the choice of the fundamental units $\eta_1, \ldots, \eta_{d-1}$. As $b \in \mathbb{Z}^d$, Equation (8-1) tells us that each integral point P in $\mathcal{F}(\sigma)$ gives rise to an intersection of γ_σ with the lattice $\mathbb{Z}^d$. Thus our algorithm will essentially (up to numerical issues) do the following.

(1) For each $\sigma \in \Sigma$, compute all $q_c \in [-e^{-\pi\sqrt{3}}, e^{-2\pi}] \setminus \{0\}$ for which $\gamma_\sigma(q_c) \in \mathbb{Z}^d$, and compute the corresponding j-invariants.

(2) For each such j and additionally all $j \in \{1, 2, \ldots, 1727\}$: if $j \in \mathbb{Z}$, compute the image type of an associated mod-p Galois representation.

(3) If furthermore the image of the representation is contained in the normalizer of a nonsplit Cartan subgroup, then output j.

An explicit bound for $|q_c|$ and first reductions. In Section 9 we bound $|q_c|$ away from zero, and explain how this bound can be considerably improved using a classical reduction procedure going back to Baker and Davenport [1969].

Sieving for lattice points in the remaining parts of γ_σ. After having applied the first reductions, we are left with considering two compact real intervals $I_+ \subset \mathbb{R}_{>0}$ and $I_- \subset \mathbb{R}_{<0}$ of q_c-parameters. In Section 10 we will cover $\gamma_\sigma(I_+ \cup I_-)$ with ellipsoids of small volume and then use the Fincke–Pohst algorithm in order to obtain only a few remaining candidates for $j(P)$, which then can be checked in the extra search.

Extra search. A small set of values $j(P) \in \mathbb{Z}$ can be checked separately by simply computing the image type of the corresponding mod-p Galois representation, see Section 10B. We call this the extra search.

Computing the initial bound for $|q_c|$ is very fast. Starting from this bound, in principle we could use the sieve from Section 10 immediately without the first reductions from Section 9. However the latter makes simpler estimates that require much less precision and are thus considerably faster. When the first reduction method cannot continue further, the sieve using ellipsoids sieves away many candidates for $j(P)$. Only at the end, for large $|q_c|$, the sieve eventually stops sieving away a lot of false candidates. At this point it becomes beneficial to simply use the extra search, as only a few values for $j \in \mathbb{Z}$ remain that correspond to those q_c.

Remark 8.1 (taking care of numerical issues). Our algorithm needs to deal with real numbers. A curious and trivial fact is that all real numbers in this paper (although $\mathbb{R}$ is uncountable) are exactly representable in a computer; however only symbolically, not as floating point numbers or more generally as rational numbers. To do efficient computations we need to work with rational approximations instead. Thus dealing with error estimates is unavoidable. To solve all arising numerical problems elegantly, we used throughout *interval arithmetic*, where a real number x is replaced by an interval $[a, b]$ with $a, b \in \mathbb{Q}$, containing x. This has the advantage that at each step of the algorithm we have exact rational bounds for the computed real numbers. If at some point during runtime it turns out that these bounds are too weak, we simply rerun the relevant parts of the program with larger and larger precision, that is, we represent the initial real numbers x by shorter and shorter intervals $[a, b]$. This will certainly increase the running time as the heights of a, b will increase. But once the precision of the result is sufficient, we are certain that the obtained bounds are correct.

Note also that whenever we found a lattice point on γ_σ, we need to know which q_c-parameter it comes from in order to determine the possible values of $j(P)$. Solving this equation to a high precision can be very costly timewise, which is why the first reductions and the subsequent sieving steps are so important.

9. Baker's bound and its reduction

In this section we bound $q_c(P)$, using the bound for $|j(P)|$ obtained in [Bajolet and Sha 2014] with Baker's method. Afterwards, we show how it can be improved using the method of Baker and Davenport [1969].

Theorem 9.1. *Assume that $p \geq 7$. Let δ be the smallest divisor of $(p-1)/2$ satisfying $\delta \geq 3$. Set*

$$\mho = 30^{\delta+5}\delta^{-2\delta+4.5}p^{6\delta+5}(\log p)^2, \quad \mho_0 = \log(e^{\mho} + 2079)$$

Then for any integral point P on $X_{\mathrm{ns}}^+(p)$ with nearest cusp c we have

$$\log|j(P)| < \mho \quad and \quad \log|q_c(P)^{-1}| \leq \mho_0.$$

Proof. The first statement is a version of Theorem 1.1 of [Bajolet and Sha 2014]. The second statement follows from the first one using (2-16). $\qquad\square$

Remark 9.2. Modular units used in [Bajolet and Sha 2014] are not "economical" (in the sens of this article). Using instead economical units would yield a slightly sharper bound than $\mho_0$. However, the quality of this bound is not of significant importance for the subsequent reduction process. Therefore we prefer to use the "prêt à porter" result from [Bajolet and Sha 2014] rather than repeat the (rather technical) argument from that paper replacing the "naive" units used therein by economical ones.

We call $\mho_0$ *Baker's bound.* It is usually numerically huge (around 10^{100} for small p and even about 10^{1000} for $p = 97$), and so are the implied bounds for the exponents $b_0, \ldots, b_{d-1}$, that can be obtained using (7-8); therefore they are not suitable for direct enumeration of all possible vectors $b = (b_0, \ldots, b_{d-1})$. Moreover, checking whether such a candidate vector b comes from an integral point P is nontrivial and computationally expensive.

However, in practical situations the bound $\mho_0$ can be drastically reduced, using the numerical Diophantine approximations technique introduced by Baker and Davenport [1969] and developed in [Bilu and Hanrot 1996; Tzanakis and de Weger 1989] in the context of the Diophantine equation of Thue.

As in the previous section we fix a cusp c and consider integral points $P \in \Omega_c$. We shall usually omit the index c, writing $\delta_{c,k} = \delta_k$ and $\vartheta_{c,k} = \vartheta_k$ for the quantities defined in (7-5).

As we have seen in Remark 7.1, at least one of the numbers $\delta_1, \ldots, \delta_{d-1}$ is nonzero. To simplify notation we will assume that $\delta_1 \neq 0$. We denote

$$B_0 = |\delta_1|\mho_0 + |\vartheta_1| + \Theta,$$

so that $|b_1| \leq B_0$ by (7-8).

Put

$$\delta = \frac{\delta_2}{\delta_1}, \quad \lambda = \frac{\delta_2 \vartheta_1 - \delta_1 \vartheta_2}{\delta_1}.$$

Relation (7-7) implies that

$$|b_2 - \delta b_1 + \lambda| \leq (1 + |\delta|) \Theta |q_c(P)|^{1/p}, \tag{9-1}$$

which gives us up to λ a good rational approximation of δ. The idea is to find by continued fraction expansion of δ an integer r such that $r\delta$ is close to an integer but $r\lambda$ is not, which then gives us a better upper bound for $\log |q_c(P)^{-1}|$. For this, we proceed as follows. We fix a real number $T \geq 2$ (in our computations we initially take $T = 10$). Next, using continued fractions we find a "good" rational approximation of δ; precisely, we find a nonnegative integer $r \leq T B_0$ such that

$$\|r\delta\| \leq (T B_0)^{-1}$$

where $\|\cdot\|$ is the distance to the nearest integer. Thus, T controls the precision of this rational approximation on top of B_0. Now, if $r\lambda$ is not "very close" to the nearest integer (in practice if $\|r\lambda\| \geq 2T^{-1}$) then we can bound $|q_c(P)^{-1}|$. Indeed, multiply both sides of (9-1) by r. The right-hand side of the resulting inequality will be bounded from above by $(1 + |\delta|) \Theta T B_0 |q_c(P)|^{1/p}$, and the left-hand side would be

$$|rb_2 - r\delta b_1 + r\lambda| \geq \|r\lambda\| - B_0 \|r\delta\| \geq \|r\lambda\| - T^{-1},$$

since $|b_1| \leq B_0$. This gives the following upper bound for $|q_c(P)^{-1}|$:

$$\log |q_c(P)^{-1}| \leq p \log \frac{(1 + |\delta|) \Theta T B_0}{\|r\lambda\| - T^{-1}} =: \mho_1. \tag{9-2}$$

In the case when $\|r\lambda\| < 2T^{-1}$ we increase T (in our computations we replace it by $10T$) and restart, until $\|r\lambda\| \geq 2T^{-1}$. In practice only very few such iterations are needed: Heuristically, $\|r\lambda\|$ can be thought of a random number in $[0, 1]$ (with respect to the Lebesgue measure), and thus a particular T works with "probability" $1 - 2T^{-1}$. As $\log(T B_0)$ is almost $\log(B_0)$, the precise value of T is not that important.

Since $\mho_1$ depends logarithmically on $\mho_0$, it is expected to be much smaller than $\mho_0$, and in practice it is.

We then repeat the same procedure, but this time with $\mho_1$ instead of $\mho_0$, obtaining for $\log |q_c(P)^{-1}|$ a new reduced bound $\mho_2$, and so on. We stop this reduction process once it does not improve the previous bound on $\log |q_c(P)^{-1}|$ by more than 1%. In practice, three to four iterations of this procedure suffice for that. We call $\widehat{\mho}$ the obtained reduced bound for $\log |q_c(P)^{-1}|$. In practice $\widehat{\mho}$ is around 200 for small p and about 2200 for $p = 97$.

Remark 9.3 (geometry intuition behind the reduction process). Recall from Section 8 that we are interested in the real q_c-parameters $q_c \in I_0$ at which $\gamma_\sigma(q_c)$ is a lattice point $b \in \mathbb{Z}^d$. For $|q_c| \to 0$ the ℓ_2-norm of γ_σ tends to infinity, and the asymptotic direction of γ_σ is given by the vector $(\delta_0, \ldots, \delta_{d-1})$, compare with Remark 7.1. Moreover, the Baker bound $\mho_0$ for $\log |q_c^{-1}|$ together with (7-8) restricts our search to a certain hypercube in $\mathbb{R}^d$. In informal, more geometric terms, the reduction procedure can be

described as follows. We project γ_σ to its first two coordinates, and we try to find a large part of the domain of γ where this projection does not intersect the lattice points $\mathbb{Z}^2 \subset \mathbb{R}^2$. For this we approximate the slope of the projected γ_σ by a rational number; in other words we make a change of coordinates via a matrix in $\mathrm{GL}_2(\mathbb{Z})$, sending $\mathbb{Z}^2$ to $\mathbb{Z}^2$, such that the projected γ_σ becomes asymptotically almost horizontal. That is, the vertical coordinate changes asymptotically very slowly, which means that it stays over a large part of the domain between two integers. Then using the error bounds of (7-7) we deduce a new upper bound $\mho_1$ for $\log |q_c^{-1}|$.

10. Sieving lattice points on γ_σ

10A. *Ellipsoid sieve.* We continue with the set-up of Section 8. For notational simplicity, we don't keep $\sigma \in \Sigma$ and c in the notation. That is, we write λ for λ_σ, γ for γ_σ, and q for q_c. Suppose that we want to find all q in a certain interval within the domain of γ at which $\gamma(q) \in \mathbb{Z}^d$.

One serious numerical problem is, that we can compute the modular units U, and thus γ, only up to an arbitrary finite precision, but never exactly. Moreover, a better precision (i.e., a better error bound) requires longer running time and more memory consumption. Thus we are looking for ways to algorithmically bound γ in such a way that only very few candidates j remain. For this we use two different methods:

(1) We will cover (the image of) γ with exactly computed ellipsoids, such that each of the ellipsoids intersects $\mathbb{Z}^d$ in very few points, which can be determined using an enhanced version of the algorithm of Fincke and Pohst [1985].

(2) If a subinterval I of the domain of γ has the property, that the restriction $\gamma|_I$ has a coordinate with provably positive or negative derivative, we can use the bisection method or Brent's method [1971] to compute all q for which this coordinate is integral.

By default we try to use the first of the two methods, because it is considerably faster in most situations. Only at places where γ intersects $\mathbb{Z}^d$ or is very close to doing so, the second method becomes preferable. Next we discuss both these two methods in detail.

Covering $\gamma(I)$ with one ellipsoid. Let $I = [q_1, q_2] \subset \mathbb{R} \setminus \{0\}$ be an interval in the domain of γ. Recall that $U = u_{\mathcal{O}}$ is a product of Siegel functions g_a (Theorem 6.1), whose leading terms come from the factors in front of the infinite products in (4-2). Therefore the leading term of $\log |U|$ is affine linear in τ.

The remainder of $\log |U|$ is an infinite sum, which can be estimated by a finite sum plus an error term, see Corollary A.4 in the Appendix. We use real and complex interval arithmetic, using that q lies in the given interval I, and obtain constant lower and upper bounds for the remainder of $\log |U|$ that hold for all τ in the interval given by $q \in I$.

As the coordinates of λ are sums of terms $\log |U|$, it follows that the image of $\lambda|_I$ lies in the Minkowski sum of a line segment (coming from the leading terms of the terms $\log |U|$) and an axis-parallel cube (coming from the remaining terms of the summands $\log |U|$). Let us call the line segment S, and the cube C. Thus, $\lambda(I) \subseteq S + C$, where "+" denotes the Minkowski sum. We look for an ellipsoid E of small volume that contains $S + C \supseteq \lambda(I)$. For this we need some preparation.

Let Q be a symmetric positive definite $d \times d$ matrix, which gives rise to a quadratic form on $\mathbb{R}^d$. In the following we write $E_Q := \{x \in \mathbb{R}^d \mid x^t Q x \leq 1\}$ for its unit ball, which is a euclidean ellipsoid.

Lemma 10.1 (product of ellipsoids). *Let Q_1, Q_2 be positive definite matrices giving rise to quadratic forms on $\mathbb{R}^{d_1}$ and $\mathbb{R}^{d_2}$, respectively. Then the ellipsoid E_Q of smallest volume containing $Q_1 \times Q_2$ is given by the block-diagonal matrix Q with the two blocks $(d_1/(d_1 + d_2))Q_1$ and $(d_2/(d_1 + d_2))Q_2$.*

Lemma 10.2 (projecting ellipsoids). *Let Q be a positive definite $d \times d$ matrix. Let P be a $d' \times d$ matrix of rank d' representing a linear surjection $\mathbb{R}^d \to \mathbb{R}^{d'}$. The image of E_Q under P is given by $P(E_Q) = E_{Q'}$ with $Q' = (P Q^{-1} P^t)^{-1}$.*

Proposition 10.3 (convex hulls of ellipsoids). *Let Q be a positive definite $d \times d$ matrix, and let $a \in \mathbb{R}^d$ be a vector. Define $E_{Q'}$ as the ellipsoid given by $Q' = (1/(d+1))\left(\frac{1}{d}Q^{-1} + a^t a\right)^{-1}$. Then $E_{Q'}$ is an ellipsoid that contains both translates $E_Q + a$ and $E_Q - a$ of E_Q.*

Proof. Let P be the $d \times (d+1)$ matrix $(\mathrm{id}_d \mid a)$, i.e., a $d \times d$ identity matrix with an augmented column given by vector a. The convex hull of $E_Q + a$ and $E_Q - a$ can be written as $P(E_Q \times [-1, +1])$. Note that $[-1, +1] = E_{\mathrm{id}_1}$, where id_1 is the 1×1 identity matrix. Using Lemma 10.1 we find an ellipsoid $E_{\widetilde{Q}}$ containing $E_Q \times [-1, +1]$, namely the one given by a block matrix $\widetilde{Q}$ with a $d \times d$ block $(d/(d+1))Q$ and a 1×1 block with entry $1/(d+1)$. Define Q' as in Lemma 10.2 such that $P(E_{\widetilde{Q}}) = E_{Q'}$. Then one quickly checks that Q' is given as in the assertion of the proposition, i.e., $Q' = (1/(d+1))\left(\frac{1}{d}Q^{-1} + a^t a\right)^{-1}$, and we have

$$E_Q \pm a \subseteq \mathrm{conv}(E_Q - a, E_Q + a) = P(E_Q \times [-1, +1]) \subseteq P(E_{\widetilde{Q}}) = E_{Q'}. \qquad \square$$

Now let us return to the problem of finding an ellipsoid E containing $S + C \supseteq \lambda(I)$. It is easy to write down the ellipsoid E_C of smallest volume that contains C; one can obtain it by iterating Lemma 10.1, using that C is a product of 1-dimensional ellipsoids. By translating the coordinate system, we may assume that the segment S is centered at the origin, its endpoints being $\pm a$. Then Proposition 10.3 yields an ellipsoid that contains both $E_C \pm a$, and thus $S + C$, and thus also $\lambda(I)$.

As $\gamma(I) = A \cdot \lambda(I)$ is just an affine image of $\lambda(I)$, with Lemma 10.2 we obtain immediately an ellipsoid containing $\gamma(I)$. Let us call this ellipsoid E_I.

Computing lattice points on $\gamma(I)$. We are interested in the q-parameters such that $\gamma(q) \in \mathbb{Z}^d$.

For this, in the previous section we computed an ellipsoid $E_I \supseteq \gamma(I)$. With the Fincke–Pohst algorithm, one can compute all lattice points in an ellipsoid E_I. We note that one needs to adjust the original Fincke–Pohst algorithm in two ways.

(1) As the dimensions d become relatively high (say larger than 8), it is in practice necessary to first LLL-reduce the basis of the lattice with respect to the quadratic form that defines the ellipsoid. Otherwise the Fincke–Pohst algorithm can become too slow.

(2) Our ellipsoid E_I is in general not centered at a lattice point; whereas the original Fincke–Pohst algorithm is for ellipsoids centered at the origin. This generalization is indeed not difficult to implement (see for example our source code for our precise implementation).

Note that everywhere in the code we use interval arithmetic. That is, our computations do not compute the exact real numbers, but instead exact intervals in which the correct results of the computations lie; compare with Remark 8.1. In the Fincke–Pohst algorithm this ensures that we get indeed all lattice points in E_I, and possibly a few more "false candidates." The higher the underlying precision is that we are using, the fewer false candidates there will be.

Examining lattice points on $\gamma(I)$. Having computed the lattice points $E_I \cap \mathbb{Z}^d$ (plus possibly some false candidates), there are basically two possibilities:

(1) It may happen that Fincke–Pohst returns no lattice point. Then we have a proof that $E_I \cap \mathbb{Z}^d$ is empty, and hence $\gamma(I) \cap \mathbb{Z}^d$ is empty. Thus $X_{ns}^+(p)$ contains no integral point within the hyperbolic triangle $\mathcal{F}(\sigma)$ with q-parameter in I.

(2) It may happen that Fincke–Pohst returns at least one lattice point.

(a) One way to continue is to split I into two smaller intervals $I = I_1 \cap I_2$ and continue with I_1 and I_2 recursively. The intuition is that the corresponding ellipsoids E_{I_1} and E_{I_2} should be of much smaller volume and should thus contain fewer lattice points. In the current implementation we do exactly this when Fincke–Pohst returns at least two lattice points, and we split I into two equal pieces I_1 and I_2 in the logarithmic scale (which is a good splitting point in practice; it corresponds to bisecting the interval in τ-coordinates).

(b) When Fincke–Pohst returns exactly one lattice point v, it may happen that it lies actually on $\gamma(I)$ and which we will not get rid of by splitting I into smaller pieces. Thus we try to compute which j-invariant(s) it corresponds to. This is nontrivial for numerical reasons. Our implementation does the following. We compute the derivative of $\gamma|_I$ in interval arithmetic. If in this way we cannot prove that at least one coordinate of $\gamma|_I$ has everywhere positive or everywhere negative derivative, we continue as in (a) by splitting I into two pieces and go deeper into the recursion. Otherwise we know that one coordinate, say the k-th one, is strictly monotone. In particular, $\gamma|_I$ may go through the obtained lattice point v at most once. Then we use the bisection method (as always in interval arithmetic) to find the q-parameter (well, only an interval I_q that contains this q-parameter) such that the k-th coordinates satisfy $\gamma_k(q) = v_k$. It may happen that γ_k is larger (or smaller) than v_k at both endpoints of I, in which case we also proved that $\gamma(I) \cap \mathbb{Z}^d$ is empty. Having found I_q, we compute in interval arithmetic $\gamma(I_q)$, which is a vector whose coordinates are all real intervals, i.e., $\gamma(I_q)$ is a cube. We check whether it contains the obtained lattice point v. If not, again we know that $\gamma(I) \cap \mathbb{Z}^d$ is empty. Otherwise, we compute the set of all integral values for j that correspond to q-parameters in I_q. If there are no such integral values for j, we are of course again finished. If there is only one such value for j, we test it in the extra search, see Section 10B. However if there are more than one such value, we increase the precision of our computations, and rerun the bisection method that computes the real interval I_q, until at some point I_q is small enough.

Remark 10.4. In an earlier version of this paper (see the first preprint version on the arXiv) we did not cover γ by ellipsoids. Instead, in the language of this section, we concentrated on one of the coordinates

γ_i of γ and solved $\gamma_i(q) = k$ for all integral values of k within the range that is left after the first reductions of Section 9. The ellipsoid method has two advantages: Firstly, for q close to zero it is faster, as a single ellipsoid can cover many choices for k. In principle one could even replace the first reductions from Section 9 by suitable ellipsoids,[5] however the above reduction is much faster as it requires little precision. Secondly, solving $\gamma_i(q) = k$ for q runs into considerable numerical issues, especially for larger $|q|$ due to slow convergence. This being said, if done right, a coordinatewise method might be a way to improve on our algorithm in the future, in particular as a middle step between the ellipsoid approach and the extra search, where the largest running time improvements are possible.

10B. *Extra search.* Assume that it only remains to verify for a few values for $j(P) \in \mathbb{Z}$, whether they come from an integral point P. In practice, these values will contain the numbers $1, 2, \ldots, 1727$, which come from potential integral points with nonreal q_c-parameter. Moreover it will contain the values of j that could not be excluded during the sieve of Section 10, as well as all $j \in \mathbb{Z}$ with $|j| \le j_0$ for some j_0 such as $j_0 = 2^{16}$ (or even larger for big p), as for small j the sieve is slower than the direct extra search described below. Also, the sieve has to be performed for each $\sigma \in \Sigma$, and the set Σ is of cardinality $p(p-1)/2$, quite a big number for big p.

Recall that to an elliptic curve $E/\mathbb{Q}$ and a prime number p we associate a Galois representation

$$\rho_{E,p} : \mathrm{gal}_{\mathbb{Q}} \to \mathrm{GL}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p),$$

which is defined by the natural action of the absolute Galois group $G_{\mathbb{Q}}$ on the torsion group $E[p]$. Points in $X_{\mathrm{ns}}(p)(\mathbb{Q})$ correspond to the elliptic curves $E/\mathbb{Q}$ such that the image of $\rho_{E,p}$ is contained in the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

It is known that, if this latter property holds for some elliptic curve $E/\mathbb{Q}$ with $j(E) \ne 0, 1728$, then it holds for any quadratic twist of E, that is, for any other elliptic curve E' with $j(E') = j(E)$. Indeed, E' is isomorphic to E over some field K of degree at most 2. Denote by χ_K the character of $G_{\mathbb{Q}}$ corresponding to K. Then $\rho_{E',p} = \rho_{E,p}\chi_K$. Hence if the image of $\rho_{E,p}$ is contained in the normalizer of a nonsplit Cartan subgroup, then so is the image of $\rho_{E',p}$.

Hence, if we fix $j \in \mathbb{Q}$, distinct from 0 and 1728, then, to verify whether $X_{\mathrm{ns}}^+(p)$ has a rational point P with $j(P) = j$, it suffices to verify for at least one curve $E/\mathbb{Q}$ with $j(E) = j$ whether the image of $\rho_{E,p}$ is contained in the normalizer of a nonsplit Cartan subgroup. This can be readily accomplished within [Sage-Math 2017] using the functions $E = EllipticCurve\_from\_j(j)$ and $E.galois\_representation().image\_type(p)$.

10C. *Running time of the algorithm.* In order to obtain Theorem 1.1, we let our algorithm run for all primes $7 \le p \le 97$ in parallel on the PlaFRIM computer cluster. For any such p, let t denote the running time in seconds multiplied by the number of CPUs that were in use; see Table 2. Thus, t is an upper bound for the time in seconds that our algorithm would take for a prime p on a single CPU. The computation for $p = 79$ had the highest running time of almost 3.5 CPU years. The total running time was almost 16 CPU years.

---

[5]This is analogous to the situation for S-unit and Mordell equations, where one can replace the classical first reduction of the initial height bound by ellipsoids [von Känel and Matschke 2016].

p	t	t/p^4	p	t	t/p^4	p	t	t/p^4	p	t	t/p^4
7	$6.7 \cdot 10^3$	2.76	29	$2.4 \cdot 10^5$	0.34	53	$4.3 \cdot 10^6$	0.55	79	$1.2 \cdot 10^8$	2.83
11	$6.8 \cdot 10^3$	0.47	31	$8.3 \cdot 10^5$	0.90	59	$1.3 \cdot 10^7$	1.03	83	$6.1 \cdot 10^7$	1.28
13	$2.9 \cdot 10^4$	1.01	37	$1.8 \cdot 10^6$	0.94	61	$1.8 \cdot 10^7$	1.24	89	$1.0 \cdot 10^8$	1.59
17	$2.8 \cdot 10^4$	0.33	41	$1.2 \cdot 10^6$	0.41	67	$3.0 \cdot 10^7$	1.47	97	$6.2 \cdot 10^7$	0.70
19	$1.2 \cdot 10^5$	0.89	43	$2.7 \cdot 10^6$	0.77	71	$2.6 \cdot 10^7$	1.01			
23	$9.0 \cdot 10^4$	0.33	47	$2.0 \cdot 10^6$	0.40	73	$6.9 \cdot 10^7$	2.42			

Table 2. Running times t in CPU seconds for computing $X_{\mathrm{ns}}^+(p)(\mathbb{Z})$.

For each $p \neq 97$ the computation was based on the field $K = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. For $p = 97$ we took for K instead the subfield of degree 16, as during a test-run on a single hyperbolic triangle $\mathcal{F}(\sigma)$ this choice improved the running time by a factor of 4.5. The running time for $p < 100$ in our computations seems to grow slightly faster than p^4, but as for the asymptotic complexity for our algorithm this is a strict underestimate. A p^2 factor already comes from the number of hyperbolic triangles $\mathcal{F}(\sigma)$ that cover $X_{\mathrm{ns}}^+(\mathcal{C})$ over which the algorithm iterates. For each $\mathcal{F}(\sigma)$, the bottleneck (at least in the current range) is the computation of integral points in the ellipsoids. For each such ellipsoid, the Fincke–Pohst algorithm needs to be applied to an LLL-reduced quadratic form (otherwise it becomes impractical for moderately large d), and it also needs $O(d^3)$ time to compute the Fincke–Pohst form of the ellipsoid. Moreover the number of covering ellipsoids and their required numerical precision is hard to estimate a priori, which makes even an upper bound for the running time of our algorithm currently out of reach.

Note that we did not prove that the algorithm actually terminates. Something very special would need to happen for it not to terminate, such as the existence of an integral point out of the reach of the extra search at which the derivative of γ vanishes. In any case, if the algorithm will not terminate for some larger p in the future, presumably there will be a quick fix of the program.

If the algorithm terminates then the output is proved to be correct, i.e., the obtained set of integral points on $X_{\mathrm{ns}}^+(p)$ is provably complete.

Appendix: Approximate formulas for Siegel functions, modular units and their derivatives

In this appendix we collect formulas we were using in the computation of Section 10 to numerically approximate modular units and their derivatives.

We start by approximating Siegel functions. We use notation of Section 4A.

Proposition A.1. *Let n_0 be a positive integer. Then for a nonzero $\boldsymbol{a} = (a_1, a_2) \in \mathbb{Q}^2 \cap [0, 1)^2$ and $\tau \in \mathcal{H}$ we have*

$$\log|g_{\boldsymbol{a}}(\tau)| = \ell_{\boldsymbol{a}} \log|q| + \log|\varrho_{\boldsymbol{a}}| + \sum_{\substack{n=0 \\ (n,a_1) \neq (0,0)}}^{n_0-1} \log|1 - q^{n+a_1} e^{2\pi i a_2}| + \sum_{n=0}^{n_0-1} \log|1 - q^{n+1-a_1} e^{-2\pi i a_2}|$$

$$+ O_1 \left(\frac{|q|^{n_0+a_1} + |q|^{n_0+1-a_1}}{(1-|q|)^2} \right). \quad \text{(A-1)}$$

Remark A.2. The term $\log|\varrho_a|$ vanishes unless $a_1 = 0$. In this latter case it might have been included into the first sum by omitting the condition $(n, a_1) = (0, 0)$. However, we prefer to write (A-1) as we do, because we want to separate the constant and the nonconstant terms.

Proof. The proof is similar to that of Proposition 4.5. Using the inequality $|\log(1 + z)| \le |z|/(1 - |z|)$ for $|z| < 1$, we estimate, for $n \ge 1$, the terms of the product expansion (4-2) as

$$\left|\log(1 - q^{n+\tilde{a}_1}e^{2\pi i \tilde{a}_2})\right| \le \frac{|q|^{n+\tilde{a}_1}}{1 - |q|^n}, \quad \left|\log(1 - q^{n+1-\tilde{a}_1}e^{-2\pi i \tilde{a}_2})\right| \le \frac{|q|^{n+1-\tilde{a}_1}}{1 - |q|^n}.$$

Adding this up for all $n \ge n_0$, we bound the error term in (A-1) as

$$\sum_{n=n_0}^{\infty} \frac{|q|^{n+\tilde{a}_1} + |q|^{n+1-\tilde{a}_1}}{1 - |q|} = \frac{|q|^{n_0+\tilde{a}_1} + |q|^{n_0+1-\tilde{a}_1}}{(1 - |q|)^2}.$$

This proves the proposition. $\qquad\square$

The absolute value $|g_{\tilde{a}}(\tau)|$ is 1-periodic as a function of τ. Hence it can be viewed as a function of $q = e^{2\pi i \tau}$. We need an estimate for the logarithmic q-derivative $\frac{d}{dq}\log|g_{\tilde{a}}|$.

Proposition A.3. *Let $\tilde{a}$, τ and n_0 be as in Proposition A.1. Assume that $\tau \in \overset{\circ}{\mathcal{F}}$. Then*

$$\left(\frac{d}{dq}\log|g_{\tilde{a}}|\right)(\tau) = \ell_{\tilde{a}}\operatorname{Re}\frac{1}{q} + \sum_{n=0}^{n_0-1}\operatorname{Re}\left(\frac{-(n+\tilde{a}_1)q^{n-1+\tilde{a}_1}e^{2\pi i \tilde{a}_2}}{1 - q^{n+\tilde{a}_1}e^{2\pi i \tilde{a}_2}} + \frac{-(n+1-\tilde{a}_1)q^{n-\tilde{a}_1}e^{-2\pi i \tilde{a}_2}}{1 - q^{n+1-\tilde{a}_1}e^{-2\pi i \tilde{a}_2}}\right)$$

$$+ O_1\left(\frac{n_0|q|^{n_0-1} - (n_0-1)|q|^{n_0}}{(1 - |q|)^2}\left(\frac{1}{1 - |q|^{n_0+\tilde{a}_1}} + \frac{1}{1 - |q|^{n_0+1-\tilde{a}_1}}\right)\right). \quad \text{(A-2)}$$

Proof. For any smooth function $f : \mathbb{R} \to \mathbb{C}^{\times}$, we have $\frac{d}{dx}\log|f(x)| = \operatorname{Re}(f'(x)/f(x))$. Using the product expansion (4-2), this already explains the main term in (A-2). For the O_1-term we bound

$$\operatorname{Re}\left(\frac{-(n+\tilde{a}_1)q^{n-1+\tilde{a}_1}e^{2\pi i \tilde{a}_2}}{1 - q^{n+\tilde{a}_1}e^{2\pi i \tilde{a}_2}}\right) \le \left|\frac{-(n+\tilde{a}_1)q^{n-1+\tilde{a}_1}e^{2\pi i \tilde{a}_2}}{1 - q^{n+\tilde{a}_1}e^{2\pi i \tilde{a}_2}}\right| \le \frac{(n+\tilde{a}_1)|q|^{n-1+\tilde{a}_1}}{1 - |q|^{n+\tilde{a}_1}}$$

For the denominator, we simply bound $1 - |q|^{n+\tilde{a}_1} \ge 1 - |q|^{n_0+\tilde{a}_1}$ for $n \ge n_0$. We want to bound the numerator for $n \ge n_0$ as

$$(n+\tilde{a}_1)|q|^{n-1+\tilde{a}_1} \le n|q|^{n-1}.$$

This follows from the fact that the function $x \mapsto x|q|^{x-1}$ is decreasing for $x \ge 1$ whenever $|q| < e^{-1/x}$, which is true because $\tau \in \mathcal{F}$, and then plugging into this function the two arguments $x = n$ and $x = n+\tilde{a}_1$.

Thus, for $n \ge n_0$, we obtain

$$\sum_{n=n_0}^{\infty}(n+\tilde{a}_1)|q|^{n-1+\tilde{a}_1} \le \sum_{n=n_0}^{\infty} n|q|^{n-1} = \frac{n_0|q|^{n_0-1} - (n_0-1)|q|^{n_0}}{(1 - |q|)^2}.$$

This explains the first half of the O_1-term. The other half for exponent $n+1-a_1$ instead of $n+a_1$ is treated in the same way. $\qquad\square$

Now it is easy to obtain a similar result for modular units.

Corollary A.4. *Let n_0 be a positive integer. Then in the set-up of Proposition 5.8, for every $P \in \overset{\circ}{\mathcal{F}}(\sigma)$ we have*

$$\log|u(P)| = \frac{\operatorname{Ord}_c u}{p} \log|q_c(P)| + \log|\varsigma_c|$$

$$+ m \sum_{n=0}^{n_0-1} \Bigg(\sum_{\substack{a \in \mathcal{O}\sigma \\ (n,a_1) \neq (0,0)}} \log\big|1 - q_c(P)^{n+\tilde{a}_1} e^{2\pi i \tilde{a}_2}\big| + \sum_{a \in \mathcal{O}\sigma} \log\big|1 - q_c(P)^{n+1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}\big| \Bigg)$$

$$+ O_1 \Bigg(m \sum_{a \in \mathcal{O}\sigma} \frac{|q_c(P)|^{n_0+\tilde{a}_1} + |q_c(P)|^{n_0+1-\tilde{a}_1}}{(1-|q_c(P)|)^2} \Bigg),$$

In addition to this,

$$\left(\frac{d}{dq_c} \log|u| \right)(P)$$

$$= \frac{\operatorname{Ord}_c u}{p} \operatorname{Re} \frac{1}{q_c(P)} + m \sum_{n=0}^{n_0-1} \sum_{a \in \mathcal{O}\sigma} \operatorname{Re}\Bigg(\frac{-(n+\tilde{a}_1)q_c(P)^{n-1+\tilde{a}_1} e^{2\pi i \tilde{a}_2}}{1 - q_c(P)^{n+\tilde{a}_1} e^{2\pi i \tilde{a}_2}} + \frac{-(n+1-\tilde{a}_1)q_c(P)^{n-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}}{1 - q_c(P)^{n+1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}} \Bigg)$$

$$+ O_1 \Bigg(m \frac{n_0|q_c(P)|^{n_0-1} - (n_0-1)|q_c(P)|^{n_0}}{(1-|q_c(P)|)^2} \sum_{a \in \mathcal{O}\sigma} \Bigg(\frac{1}{1-|q_c(P)|^{n_0+\tilde{a}_1}} + \frac{1}{1-|q_c(P)|^{n_0+1-\tilde{a}_1}} \Bigg) \Bigg).$$

Proof. As in the proof of Proposition 5.8 we may assume that $\sigma = I$ and c is the cusp represented by $i\infty$. In this case the result is an immediate consequence of Propositions A.1 and A.3. $\qquad\square$

In the program, we use the above estimate for $\log|u(P)|$ first with $n_0 = 2$, and then with larger and larger n_0 when the overall precision needs to be increased. As for the estimate for $((d/dq_c)\log|u|)(P)$, we use it only with $n_0 = 1$, which turns out to be sufficient whenever we used it. For larger p one may want to take a slightly better approximation, for instance, with $n_0 = 2$.

Acknowledgements

References

[Bajolet and Sha 2014] A. Bajolet and M. Sha, "Bounding the j-invariant of integral points on $X_{\mathrm{ns}}^+(p)$", *Proc. Amer. Math. Soc.* **142**:10 (2014), 3395–3410. MR Zbl

[Baker and Davenport 1969] A. Baker and H. Davenport, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$", *Q. J. Math. Oxford* **20** (1969), 129–137. MR Zbl

[Balakrishnan et al. 2019] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, "Explicit Chabauty–Kim for the split Cartan modular curve of level 13", *Ann. of Math.* (2) **189**:3 (2019), 885–944. MR Zbl

[Baran 2009] B. Baran, "A modular curve of level 9 and the class number one problem", *J. Number Theory* **129**:3 (2009), 715–728. MR Zbl

[Baran 2010] B. Baran, "Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem", *J. Number Theory* **130**:12 (2010), 2753–2772. MR Zbl

[Baran 2014] B. Baran, "An exceptional isomorphism between modular curves of level 13", *J. Number Theory* **145** (2014), 273–300. MR Zbl

[Bilu 1995] Yu. Bilu, "Effective analysis of integral points on algebraic curves", *Israel J. Math.* **90**:1-3 (1995), 235–252. MR Zbl

[Bilu 2002] Yu. F. Bilu, "Baker's method and modular curves", pp. 73–88 in *A panorama of number theory or the view from Baker's garden* (Zürich, 1999), edited by G. Wüstholz, Cambridge Univ. Press, 2002. MR Zbl

[Bilu and Hanrot 1996] Yu. Bilu and G. Hanrot, "Solving Thue equations of high degree", *J. Number Theory* **60**:2 (1996), 373–392. MR Zbl

[Bilu and Hanrot 1998] Yu. F. Bilu and G. Hanrot, "Solving superelliptic Diophantine equations by Baker's method", *Compos. Math.* **112**:3 (1998), 273–312. MR Zbl

[Bilu and Hanrot 1999] Yu. Bilu and G. Hanrot, "Thue equations with composite fields", *Acta Arith.* **88**:4 (1999), 311–326. MR Zbl

[Bilu and Illengo 2011] Yu. Bilu and M. Illengo, "Effective Siegel's theorem for modular curves", *Bull. Lond. Math. Soc.* **43**:4 (2011), 673–688. MR Zbl

[Bilu and Parent 2011a] Yu. Bilu and P. Parent, "Runge's method and modular curves", *Int. Math. Res. Not.* **2011**:9 (2011), 1997–2027. MR Zbl

[Bilu and Parent 2011b] Yu. Bilu and P. Parent, "Serre's uniformity problem in the split Cartan case", *Ann. of Math.* (2) **173**:1 (2011), 569–584. MR Zbl

[Bilu et al. 2001] Yu. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers", *J. Reine Angew. Math.* **539** (2001), 75–122. MR Zbl

[Bilu et al. 2013] Yu. Bilu, P. Parent, and M. Rebolledo, "Rational points on $X_0^+(p^r)$", *Ann. Inst. Fourier* (*Grenoble*) **63**:3 (2013), 957–984. MR Zbl

[Brent 1971] R. P. Brent, "An algorithm with guaranteed convergence for finding a zero of a function", *Comput. J.* **14** (1971), 422–425. MR Zbl

[Cai 2019] Y. Cai, "An explicit bound for integral points on modular curves", preprint, 2019. To appear in *Commun. Math.* arXiv

[Chen and Cummins 2004] I. Chen and C. Cummins, "Elliptic curves with nonsplit mod 11 representations", *Math. Comp.* **73**:246 (2004), 869–880. MR Zbl

[Diamond and Shurman 2005] F. Diamond and J. Shurman, *A first course in modular forms*, Grad. Texts Math. **228**, Springer, 2005. MR Zbl

[Fincke and Pohst 1985] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis", *Math. Comp.* **44**:170 (1985), 463–471. MR Zbl

[Hanrot 2000] G. Hanrot, "Solving Thue equations without the full unit group", *Math. Comp.* **69**:229 (2000), 395–405. MR Zbl

[Heegner 1952] K. Heegner, "Diophantische Analysis und Modulfunktionen", *Math. Z.* **56** (1952), 227–253. MR Zbl

[von Känel and Matschke 2016] R. von Känel and B. Matschke, "Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via Shimura–Taniyama conjecture", 2016. To appear in *Mem. Amer. Math. Soc.*. GitHub. arXiv

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

[Koo and Shin 2010] J. K. Koo and D. H. Shin, "On some arithmetic properties of Siegel functions", *Math. Z.* **264**:1 (2010), 137–177. MR Zbl

[Kubert and Lang 1975] D. Kubert and S. Lang, "Units in the modular function field, I", *Math. Ann.* **218**:1 (1975), 67–96. MR Zbl

[Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Math. Wissenschaften **244**, Springer, 1981. MR Zbl

[Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Grad. Texts Math. **112**, Springer, 1987. MR Zbl

[Lang 1995] S. Lang, *Introduction to modular forms*, 2nd ed., Grundlehren der Math. Wissenschaften **222**, Springer, 1995. MR

[Lidl and Niederreiter 1997] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encycl. Math. Appl. **20**, Cambridge University Press, 1997. MR Zbl

[Masley 1978] J. M. Masley, "Class numbers of real cyclic number fields with small conductor", *Compos. Math.* **37**:3 (1978), 297–319. MR Zbl

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl

[Miller 2015] J. C. Miller, "Real cyclotomic fields of prime conductor and their class numbers", *Math. Comp.* **84**:295 (2015), 2459–2469. MR Zbl

[PARI/GP 2017] PARI Group, PARI/GP version 2.9.2, 2017, available at http://pari.math.u-bordeaux.fr.

[Pethő and Schulenberg 1987] A. Pethő and R. Schulenberg, "Effektives Lösen von Thue Gleichungen", *Publ. Math. Debrecen* **34**:3-4 (1987), 189–196. MR Zbl

[SageMath 2017] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 7.3)*, 2017, available at https://www.sagemath.org.

[Schoof and Tzanakis 2012] R. Schoof and N. Tzanakis, "Integral points of a modular curve of level 11", *Acta Arith.* **152**:1 (2012), 39–49. MR Zbl

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects Math. **E15**, Vieweg, Braunschweig, Germany, 1989. MR Zbl

[Sha 2013] M. Sha, *Topics in elliptic and modular curves*, Ph.D. thesis, Université Bourdeaux 1, 2013, available at https://www.theses.fr/2013BOR14851.

[Sha 2014a] M. Sha, "Bounding the j-invariant of integral points on certain modular curves", *Int. J. Number Theory* **10**:6 (2014), 1545–1551. MR Zbl

[Sha 2014b] M. Sha, "Bounding the j-invariant of integral points on modular curves", *Int. Math. Res. Not.* **2014**:16 (2014), 4492–4520. MR Zbl

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lect. **1**, Iwanami Shoten, Tokyo, 1971. MR Zbl

[Siegel 1968] C. L. Siegel, "Zum Beweise des Starkschen Satzes", *Invent. Math.* **5** (1968), 180–191. MR Zbl

[Tzanakis and de Weger 1989] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31**:2 (1989), 99–132. MR Zbl

[Washington 1982] L. C. Washington, *Introduction to cyclotomic fields*, Grad. Texts Math. **83**, Springer, 1982. MR Zbl

[Yu 2007] K. Yu, "p-adic logarithmic forms and group varieties, III", *Forum Math.* **19**:2 (2007), 187–280. MR Zbl

aurelien.bajolet@gmail.com   *Lycée Jean Dautet, La Rochelle, France*

yuri@math.u-bordeaux.fr   *Institut de Mathématiques de Bordeaux, Université de Bordeaux & CNRS, Talence, France*

matschke@bu.edu   *Department of Mathematics and Statistics, Boston University, Boston, MA, United States*