Contemporary Mathematics
Volume **701**, 2018
http://dx.doi.org/10.1090/conm/701/14142

Rational families of 17-torsion points of elliptic curves over number fields

Maarten Derickx, Barry Mazur, and Sheldon Kamienny

Fumiyuki Momose is very much missed. He was a generous warm human being, with immense energy and generosity of spirit, and an extremely gifted mathematician. One of his abiding interests was rational torsion on elliptic curves over number fields, as in [**Mom84**], [**KM88**]. *This article is written in his memory.*

1. Introduction

Rational torsion points on elliptic curves present challenges that one can come back to again and again since the topic simply continues to be a source of extremely interesting diophantine issues. If E is an elliptic curve over a number field k, its Mordell–Weil group, $E(k)$, is finitely generated. Moreover, any finite subgroup of $E(k)$ is of the form $\mathbf{Z}/N\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ where N, m are positive integers with m dividing N. Ogg's Conjecture, proved thirty-five years ago, might be phrased as saying that there is no rational torsion on elliptic curves over $\mathbf{Q}$ except as directly forced by the underlying algebraic geometry. More specifically: any example of an elliptic curve over $\mathbf{Q}$ with its Mordell–Weil group containing a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ is a member of a rationally parametrized family, in the sense that the modular curve $X(N, m)$ classifying such examples is isomorphic to $\mathbf{P}^1$.

In a paper published over two decades ago, written jointly with M. Kenku, Momose inaugurated an analogous investigation of certain types of subgroups of torsion points on elliptic curves rational over quadratic fields [**KM88**]. Kenku and Momose proved the following theorem:

THEOREM 1.1. *(Kenku, Momose) For integers N that factor as a product of powers of prime numbers < 17, and for integers m dividing N the following statements are equivalent.*

1. *There exists a quadratic field k and an elliptic curve E defined over k such that $E(k)$ contains a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$.*
2. *The modular curve that classifies such torsion, $X(N, m)$, is rational or hyperelliptic.*

Following on this work, one of the authors of the present paper established general classification results for torsion in the Mordell–Weil group of elliptic curves

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G18, 14G35, 14H51.
The authors are thankful to Ken Ribet for very helpful comments regarding an early draft of this paper.

©2018 Maarten Derickx, Sheldon Kamienny and Barry Mazur

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

over quadratic fields ([**Kam92b**], [**KN12**]; for a slightly different problem regarding torsion in elliptic curves and quadratic fields, see [**LL85**]).

Nowadays, one considers even more general questions from theoretical and computational perspectives.

- We might fix N and m and ask for a structural and numerical understanding of the collection of elliptic curves defined over fields of some fixed degree d over $\mathbf{Q}$—or over a fixed base number field k—for which its Mordell–Weil group over those fields contains a subgroup isomorphic to $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.
- Or more specifically, we might ask to classify rationally parametrized families of elliptic curves defined over number fields K_t of degree d over k and which possess N-torsion points rational over K_t[1]. In particular, we might study functions of degree d on $X_1(N)$ defined over $\mathbf{Q}$.

This paper will focus on the latter type of problem[2] as related to a diophantine analysis of appropriate Brill–Noether varieties attached to the modular curves $X_1(N)$.

A substantial amount of computation has been done. Intriguing examples have been discovered ([**DvH14**], [**Hoe14**], [**Sut**], [**JKL11a**], [**JKL11b**]). In work in progress the authors of this paper will be treating a number of explicit examples related to modular Brill–Noether curves. The present expository article, focusing on 17-torsion—dedicated to the memory of Fumiyuki Momose—is a report on a piece of that work in progress.

2. Rational N-torsion over fields of degree d

Fix two positive integers (N, d) and darken the point (N, d) in the plane if there exists a *non-CM elliptic curve*[3] defined over a number field of degree $\leq d$ having an N-torsion point rational over that field; call such points (N, d) simply: **data points**. One would like to know anything that stands out in this data set: its structure and its statistics.

There are two standard ways to look for uniformity phenomena:

- *Focusing, for example, on prime torsion, fix d and let $P(d)$ be the largest prime p such that (p, d) is in the data set.*

  Specific *exact values* of $P(d)$ are known only for small d. By [**Maz77**] $P(1) = 7$. Kamienny proved that $P(2) = 13$; Parent, building on work of Kamienny, showed $P(3) = 13$. Recently, Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll [**Kam89**] showed that $P(4) = 17$, $P(5) = 19$ and $P(6) = 37$.

  For general values of d we have the (trivially obtained) lower bound

$$d^{1/2} \ll P(d)$$

[1]The word "rational," then, is used in two senses: the parameter t ranges through the k-rational points of a rational curve (over k).

[2]and even more specifically when the base field is $\mathbf{Q}$ and $N = 17$

[3]We're thankful to Andrew Sutherland who suggested that one might keep separate the study of examples of CM elliptic curves possessing rational points of order N over fields of low degree d, since they represent a very orderly collection of known examples where for each such CM-elliptic curve, d admits a linear upper bound in N—and this would simply muddle the essential data set.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

and the deep upper bounds given by Merel's Theorem tellling us that $P(d) < \infty$. More specifically, Merel [**Mer96**] (and Oesterlé, Parent [**Par03**]) proved, for general d that

$$P(d) \leq (1 + 3^{d/2})^2,$$

so we have:

$$d^{1/2} \ll P(d) \ll 3^d.$$

We don't even seem yet able to come up with much more precise conjectures for the qualitative behavior and/or the volatility of $P(d)$. Is $P(d)$ bounded by a constant times d^A for any $A > 1/2$? Or for *some* finite value of A? Or does it grow more rapidly than that?

Consider the 'minimalist' attitude that any *interesting* diophantine phenomenon occurs no more often than would be predicted by general structural constraints. This viewpoint seems to lead to firmly believed conjectures, for example, for statistics regarding ranks of Mordell–Weil groups. This general viewpoint might also suggest the guess that $P(d) \ll d^A$ for any $A > 1/2$. But we don't seem to have enough experience yet to give any firm conjectures[4].

Here below is a graph computed by the first author of the present article jointly with Mark van Hoeij. It is a log-log plot where the axes are $(x, y) = (\log p, \log d)$, the data points recording examples of 'lowest' degree d for the corresponding p occurs as prime torsion in a non-CM elliptic curve (over a field of degree d). The quotation-marks around the word 'lowest' is meant to signal that the blue data points and the blue extrapolated line corresponds to the lowest d for which there is a rational family of such examples of prime torsion p over fields of degree d. The red data points correspond to the sporadic points. The green curve is the proved (exponential) lower bound relating d to p. Visibly, much more computation needs to be done if we are to be able to surmise any general behavior with some feeling that there is evidence behind our guess. We should note that this graph is the result of a computation, and is only proved to be complete for $p \leq 37$.

- *Fix N and let $D(N)$ be the smallest integer d such that (N, d) is in the data set.*

In contrast to our knowledge of the asymptotics of $P(d)$, with $D(N)$ we are in slightly better shape. There is a clear *cut-off* for $D(N)$: namely, $D(N) \leq \gamma_{\mathbf{Q}}(N)$ where $\gamma_{\mathbf{Q}}(N)$ is the $\mathbf{Q}$-*gonality*[5] of the modular curve $X_1(N)$. The basic $\mathbf{Q}$-parametrization $X_1(N) \to X(1) \simeq \mathbf{P}^1$ already gives us $\gamma_{\mathbf{Q}}(N) \leq \Phi(N)\Psi(N)/2$—where $\Phi(N)$ is the Euler phi function and

$$\Psi(N) = \Psi(\prod p_i^{e_i}) = \prod (p_i + 1) p_i^{e_i - 1}.$$

[4]Some conjectures in the literature give upper bounds for primes of torsion in elliptic curves of degree d, but since these published conjectures also include CM elliptic curves which our "$P(d)$" doesn't register, those conjectures necessarily must allow for an essentially linear lower bound. Specifically, see [**CCS13**] and [**LR13**].

[5]See The Appendix, Section 7 below.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

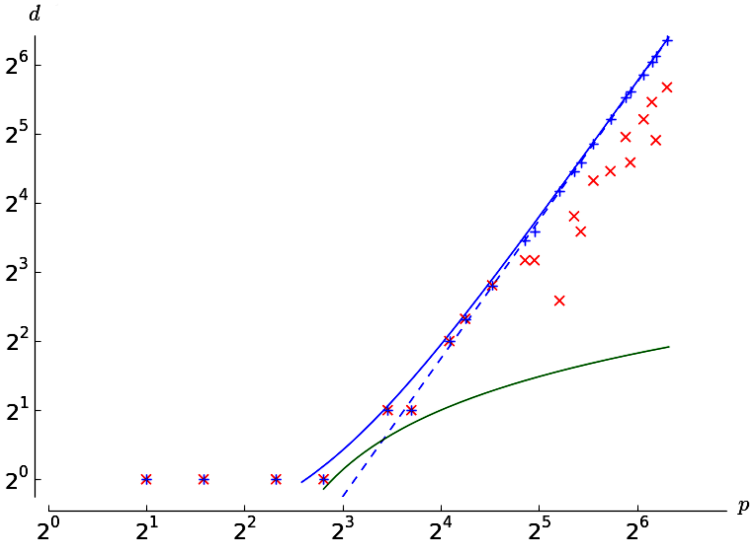

FIGURE 1. Smallest degree d such that $Y_1(p)$ has a point of that degree

In particular, we have $\gamma_{\mathbf{Q}}(N) \ll N^2$. For a discussion of the concept of gonality, see [**Abr96**], [**DvH14**] and Section 7 below.

If $d = \gamma_{\mathbf{Q}}(N)$, or more generally if there exists an $f : X_1(N) \to \mathbf{P}^1$ of degree d, then not only are there elliptic curves over fields of degree d with rational N-torsion over those fields, but there are infinitely many of them parametrized by a subset of $\mathbf{P}^1(\mathbf{Q})$. See Abramovich's basic paper [**Abr96**] where he proves the inequality

$$\frac{21}{200}(g-1) \leq \gamma_{\mathcal{C}}(N) \leq (g+3)/2,$$

where $\gamma_{\mathcal{C}}(N)$ is the $\mathbf{C}$-*gonality*, and $g \approx N^2$ is the *genus*, of $X_1(N)$. For more elementary reasons

$$\gamma_{\mathcal{C}}(N) \leq \gamma_{\mathbf{Q}}(N) \leq g+1.$$

For the $\mathbf{Q}$-gonalities of the modular curves $X_1(N)$ with $N \leq 40$ see [**DvH14**]. In particular

$N = p$	13	17	19	23	29	31	37
$\gamma_{\mathbf{Q}}(N)$	2	4	5	7	11	12	18

We will be considering data points (N, d) only for degrees $d \leq \gamma_{\mathcal{C}}(N)$. We will call an elliptic curve defined over a field of degree d possessing an N-torsion point rational over that field **sporadic** if $d = \gamma_{\mathcal{C}}(N)$ and it is *not* a member of a $\mathbf{Q}$-rationally parametrized rational family of such elliptic curves defined over fields of degree d possessing N-torsion points rational over those fields. We call it **very sporadic** if $d < \gamma_{\mathcal{C}}(N)$.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

Very sporadic data points exist. Here is a list of some known examples:

d	N	$\gamma_{\mathcal{C}}(N)$	$Reference$
3	21	4	[**Naj16**]
9, 10	29	11	[**Hoe14**]
9, 10, 11	31	12	[**DvH14**]

A result of Pete L. Clark, Brian Cook and James Stankewicz (which builds on the work of Dan Abramovich) [**CCS13**] implies that for a prime $p \geq 5$ there are at most finitely many points on $X_1(p)$ with degree $< \frac{7}{3200}(p^2-1)$. Related to this, see [**Fre94**].

3. Brill–Noether Varieties

Let X be a smooth projective curve over a characteristic zero field k. Let $\bar{k}/k$ be an algebraic closure, and $\bar{X} := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\bar{k})$. For integers $d \geq 1$, $r \geq 0$, let

$$W_d^r(X) \subset \mathrm{Pic}^d(X)$$

denote the closed subvariety of $\mathrm{Pic}^d(X)$ (defined over k) classifying divisor classes of effective divisors D of degree d that are members of linear systems (of effective divisors of degree d) of dimension $\geq r$, or equivalently such that $h^0(X, \mathcal{O}(D)) \geq r+1$; see [**ACGH85**], [**ACG11**], [**Dol12**].

The collection of Brill–Noether varieties $\{W_d^r(X) \mid d \geq 0, r \geq 0\}$ connect in the following ways:

(1) For $r \geq 1$ we have natural inclusions $W_d^r(X) \hookrightarrow W_d^{r-1}(X) \subset \mathrm{Pic}^d(X)$.

(2) Let α be a k-rational point of X, and let

$$f_\alpha : \mathrm{Pic}^d(X) \to \mathrm{Pic}^{d-1}(X)$$

be the morphism that sends the class of a divisor D to the class of $D - [\alpha]$. For $r \geq 1$ we have a commutative diagram of k-rational maps,

$$\begin{array}{ccc} W_d^r(X) & \xrightarrow{\subset} & \mathrm{Pic}^d(X) \\ \big\downarrow{\scriptstyle f_\alpha} & & \big\downarrow{\scriptstyle f_\alpha} \\ W_{d-1}^{r-1} & \xrightarrow{\subset} & \mathrm{Pic}^{d-1}(X). \end{array}$$

Statement (2) above follows from considering the global sections of the exact sequence

$$0 \to \mathcal{O}_X(D-\alpha) \to \mathcal{O}_X(D) \to \mathcal{O}_\alpha \to 0.$$

(3) We have the natural surjection

$$\eta_d : \mathrm{Sym}^d(X) \twoheadrightarrow W_d^0(X) \subset \mathrm{Pic}^d(X). \tag{3.1}$$

which is an isomorphism when restricted to

$$\mathrm{Sym}^{d,\#}(X) := \eta_d^{-1}\big(W_d^0(X) - W_d^1(X)\big) \subset \mathrm{Sym}^d(X),$$

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

i.e., to the inverse image of the complement of $W_d^1(X)$:

$$\begin{array}{ccccc} \mathrm{Sym}^{d,\#}(X) & \xrightarrow{\subset} & \mathrm{Sym}^d(X) & & \\ \downarrow \cong & & \downarrow & & \\ W_d^0(X) - W_d^1(X) & \xrightarrow{\subset} & W_d^0(X) & \xrightarrow{\subset} & \mathrm{Pic}^d(X). \end{array}$$

In paticular $\mathrm{Sym}^d(X)$ is a desingularization of $W_d^0(X)$. In certain cases of interest (e.g., as in our analysis of $X = X_1(17)$ below) $\mathrm{Sym}^d(X)$ is a small resolution of the singularities of $W_d^0(X)$.

By Theorem (1.1) in Chapter V of [**ACGH85**] if the genus $g > 1$ of X is in the range

$$d - 1 \leq g \leq 2(d-1),$$

the Brill–Noether variety $W_d^1(X)$ is of dimension greater than or equal to $2(d-1)-g$. So, if it satisfies these conditions it can be a curve only if $2d \leq g+3$ and a surface only if $2d \leq g+4$.

We will be specifically interested in the cases $r = 0, 1$:

$$W_d^1(X) \subset W_d^0(X) \subset \mathrm{Pic}^d(X),$$

noting that a choice of k-rational point α of X will give us a (k-rational) closed immersion

$$W_d^1(X) \quad \overset{f_\alpha}{\hookrightarrow} \quad W_{d-1}^0(X) \subset \mathrm{Pic}^{d-1}(X).$$

Note: If X is a curve over k a number field, for any d, one has—applying a more general theorem of Faltings [**Fal94**]—that the set of k-rational points of $W_d^1(X)$ decomposes into a *finite* union,

$$W_d^1(X)(k) \quad = \quad \bigsqcup_j \mathcal{A}_j, \tag{3.2}$$

where, for each j, the Zariski closure of $\mathcal{A}_j$ is a translate of an abelian subvariety of $Pic^0(X)$. For a study of upper bounds for the dimension of such abelian subvarieties that may arise for given values of d, gonality, and genus, see [**AH91**].

3.1. The canonical involution v. An important case for us is when $d = g-1 \geq 0$ where g is the genus of X. In this situation we have the natural involution

$$\mathrm{Pic}^{g-1}(X) \quad \overset{v}{\cong} \quad \mathrm{Pic}^{g-1}(X)$$

defined by sending any linear equivalence class of divisors $[D]$ of degree $g-1$ to the linear equivalence class of $[K-D]$ where K is the canonical divisor of X. The involution v is 'functorially defined' and is defined over any field k over which the curve itself is defined, and commutes with any automorphism of X.

Consider the fixed locus $\mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ of the involution v. The 2^{2g} geometric points of $\mathrm{Th}(X)$ are classically referred to as theta-characteristics of X; they correspond to 'square roots' of the canonical line bundle. The finite subscheme $\mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ is a torsor over $\mathrm{Pic}^0(X)[2]$. Note that the Riemann-Roch Theorem guarantees that

$$h^0(X, \mathcal{O}(D)) = h^0(X, \mathcal{O}(K-D)), \tag{3.3}$$

so v induces an involution of $W_{g-1}^r(X)$ for any $r \geq 0$. Consider the theta divisor

$$\Theta := W_d^0(X) = W_{g-1}^0(X) \subset \mathrm{Pic}^{g-1}(X),$$

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

noting that choosing any theta-characteristic $\partial \in \mathrm{Th}(X) \subset \mathrm{Pic}^{g-1}(X)$ gives the commutative diagram

$$\begin{array}{ccccc} \Theta & \xrightarrow{v} & \Theta & \xrightarrow{\subset} & \mathrm{Pic}^{g-1}(X) \\ \downarrow{\scriptstyle -\partial} & & \downarrow{\scriptstyle -\partial} & & \downarrow{\scriptstyle -\partial} \\ \Theta - \partial & \xrightarrow{-1} & \Theta - \partial & \xrightarrow{\subset} & \mathrm{Pic}^{0}(X), \end{array}$$

the theta divisors, $\{\Theta - \partial \subset \mathrm{Pic}^0(X)\}$ for the theta-characteristics ∂ ranging through $\mathrm{Th}(X)(\bar{k})$ being—each of them—symmetric under multiplication by -1 in $\mathrm{Pic}^0(X)$ and the set of them being a torsor under the group $\mathrm{Pic}^0(X)[2]((\bar{k}))$.

Note, as well, that $W^1_{g-1}(X) \subset \Theta$ is stable under the involution v as can be seen from (3.3).

3.2. Basic Brill–Noether varieties. For X a curve defined over k, denote by $\gamma = \gamma_{\bar{k}}$, its $\bar{k}$-gonality. Call $WX := W^1_\gamma(X)$ the **Basic Brill–Noether variety** attached to X. Given a k-rational point α of X, we obtain an immersion

$$WX = W^1_\gamma(X) \overset{f_\alpha}{\hookrightarrow} W^0_{\gamma-1}(X) = \mathrm{Sym}^{\gamma-1}(X) \subset \mathrm{Pic}^{\gamma-1}(X).$$

3.3. The Basic Brill–Noether variety attached to $X_1(N)$. Consider the basic Brill–Noether variety $WX_1(N) := W(X_1(N))$. Thanks to the functorial nature of Brill–Noether varieties, the automorphism group of $X_1(N)$ viewed as finite group scheme over $\mathbf{Q}$ acts naturally on $WX_1(N)$. Thus we have the group Δ of diamond operators acting $\mathbf{Q}$-rationally on $WX_1(N)$, and the w-operators acting $\mathbf{Q}(\mu_N)^+$-rationally. When N is a prime number all these operators fit into a dihedral group that act $\mathbf{Q}(\mu_N)^+$-rationally on $WX_1(N)$.

3.4. Basic Brill–Noether curves attached to algebraic curves of genus 5 and gonality 4. *Assume from now on that X is a curve defined over $\mathbf{Q}$ of genus 5 and has $\mathbf{Q}$-gonality equal to $\mathcal{C}$-gonality $\gamma = 4$.*[6]

In this case the Basic Brill–Noether variety, $W := WX$, is a curve defined over $\mathbf{Q}$ (possibly reducible). We'll refer to it as the the Basic Brill–Noether curve attached to X. An application of Clifford's Theorem [7] guarantees that $h^0(X, \mathcal{O}_X(D)) \leq 2$ for any effective divisor D of degree 4, so $W^2_4(X)$ is empty. That is, the complete linear series that corresponds to any point in the Basic Brill–Noether curve attached to X is parametrized by a pencil.

By Lemma 7.1 of Section 7, a k-rational point of WX gives us a k-linear parametrization classof maps $X \to \mathbf{P}^1$ of degree $\gamma_{\bar{k}}(X)$, and conversely. So we have

[6]The example we treat, $X_1(17)$, is of this form, as are $X_1(21)$, and $X_1(24)$.

[7]See page 204 of [**ACGH85**] for a discussion that covers the case of interest to us: genus =5, gonality and degree =4.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

PROPOSITION 3.1. *Let* $\mathrm{Aut}(X)$ *denote the group of* k*-rational automorphisms of* X*. There is a one-to-one correspondence between* k*-similarity classes*[8] *of maps* $X \to \mathbf{P}^1$ *(defined over* k*) of degree* $\gamma_{\bar{k}}(X)$ *and* $\mathrm{Aut}(X)$*-orbits of* k*-rational points of the Basic Brill–Noether curve* WX*:*

$$k\text{-similarity classes} \quad \leftrightarrow \quad WX(k)/\mathrm{Aut}(X).$$

If $d < \gamma_k(X)$ then $W^1_d(X)$ is empty (Lemma 7.1 below). In the special case where $\gamma_{\bar{k}}(X) = g - 1$ we are in the situation of section 3.1 above, and we have the canonical involution v acting on $W(X)$ compatibly with its action on $\mathrm{Pic}^{g-1}(X)$ giving a commutative diagram:

$$\begin{array}{ccc} W(X) & \xrightarrow{v} & W(X) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^{g-1}(X) & \xrightarrow{v} & \mathrm{Pic}^{g-1}(X) \end{array}$$

which commutes with any automorphism of X.

Consider a canonical embedding (defined over $\mathbf{Q}$)

$$\beta : X \xrightarrow{\cong} \Gamma \subset \mathbf{P}^4.$$

Since the genus of X is $g = 5$, by a theorem of Max Noether [**ACGH85**] the curve Γ lies on $3 = (g-2)(g-3)/2$ independent quadrics in $\mathbf{P}^4$.

For ease of nomenclature in this discussion (i.e., for the rest of this section) let us strictly reserve the symbols $\mathbf{P}^4$ to mean the projective 4-dimensional space which is the ambient space of the canonical embedding above, and $\mathbf{P}^2$ to mean the projective space generated by the linear space of *those* three independent quadrics just mentioned.

In the case of our interest we will be fixing bases,

$$\omega_0, \omega_1, \omega_2, \omega_3, \omega_4$$

of the 5 dimensional space $S := H^0(X, \Omega^1(X))$ such that the projectivization of $S^\vee$ is the $\mathbf{P}^4$ above. In terms of this basis we will be stipulating three independent quadratic relations

$$\begin{aligned} e_0 &:= e_0(\omega_0, \ldots, \omega_4) \\ e_1 &:= e_1(\omega_0, \ldots, \omega_4) \\ e_2 &:= e_2(\omega_0, \ldots, \omega_4), \end{aligned}$$

generating the kernel of the natural cup product map

$$(*) \quad \mathrm{Sym}^2(S) \xrightarrow{\kappa} H^0(X, (\Omega^1(X)^{\otimes 2}),$$

and therefore representing a basis of the projective space $\mathbf{P}^2$ above.

Note that $S = H^0(X, \Omega^1(X))$ and $H^0(X, (\Omega^1(X)^{\otimes 2})$ have a natural action of $\mathrm{Aut}(X)$ with respect to which the morphism $(*)$ is equivariant.

[8] *k-similarity* is the natural notion of equivalence for k-parametrizations: two parametrizations are **k-similar** if one can be brought to the other by composition with appropriate k-isomorphisms of domain and range.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

In the cases of our particular interest S will be the space of cuspforms of weight two and the cup product above will be given by multiplication to the space of cuspforms of weight four.

3.5. Loci of singular quadrics. For the results we are now about to quote, see page 207 of [**ACGH85**].

- Let $\mathcal{V} \subset \mathbf{P}^2$ be the sub-locus of singular quadrics[9] $' \subset {}'\mathbf{P}^4$.
- Let $\mathcal{W} \to \mathcal{V}$ be the double cover determined by choosing one of the two systems of planes in these singular quadrics.
- Let
$$\mathcal{G} \overset{\text{proj}}{\to} \mathcal{W}$$
be the $\mathbf{P}^1$-bundle whose points consist of pairs $(\Pi, ')'$ where $' \in {}'\mathcal{V}$ and $\Pi \subset ''$ is a two-plane.
- Let $v : \mathcal{W} \to \mathcal{W}$ be the involution defining the covering $\mathcal{W} \to \mathcal{V}$.
- Consider the commutative diagram
$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\alpha} & \mathrm{Sym}^4(X) \\ \downarrow{\scriptstyle \text{proj}} & & \downarrow{\scriptstyle \text{proj}} \\ \mathcal{W} & \xrightarrow{\alpha} & \mathrm{Pic}^4(X) \end{array}$$
where the morphism $\alpha : \mathcal{G} \to \mathrm{Sym}^4(X)$ is characterized on points by the rule that sends $(\Pi, ')'$ of $\mathcal{G}$ to the divisor (of degree four),
$$\alpha(\Pi, ')' := \Pi \cap \Gamma \subset \Gamma,$$
the latter being construed, via the isomorphism $\beta : X \longrightarrow \Gamma$ of subsection 3.4, as an element of $\mathrm{Sym}^4(X)$. The image of α restricted to a fiber of $\mathcal{G} \overset{\text{proj}}{\to} \mathcal{W}$ runs through a complete linear system of divisors, and therefore determines a well-defined point of $\mathrm{Pic}^4(X)$, providing a characterization (on points) of the morphism $\alpha : \mathcal{W} \to \mathrm{Pic}^4(X)$.

If ever we need to specify the curve X to which these objects are related, we indicate this in the standard manner; e.g., we write $\mathcal{W} = \mathcal{W}X$, $\mathcal{V} = \mathcal{V}X$, $\mathcal{G} = \mathcal{G}X$ etc.

3.6. The canonical representation of the Basic Brill–Noether curve. Let X be a curve satisfying our running hypotheses in this section, and put $W := WX$, the *Basic Brill–Noether curve* attached to X. Recall the involution $v : W \to W$ constructed in subsection 3.2. Let $\mathcal{W} = \mathcal{W}X$ be as in subsection 3.5 above, recalling the involution $v : \mathcal{W} \to \mathcal{W}$ constructed there.

The discussion of pp. 207-210 of of [**ACGH85**] gives the following identification.

[9]Recall that the 'generic' singular quadric threefold $' \subset {}'\mathbf{P}^4$ has a unique singular point ϵ and is the cone 'at ϵ' of a (nonsingular) quadric surface given by the intersection of $''$ with any hyperplane not passing through ϵ. That quadric surface has two rulings by lines (possibly not rational over the base field k). Taking the cone through ϵ of each of these rulings gives us two 2-dimensional rulings, now, of the quadric threefold $''$ (again possibly not rational over the base field k). That is, $''$ is swept out by two pencils of planes (i.e., 2-dimensional projective linear subspaces).

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

PROPOSITION 3.2. *The image of the canonical morphism $\alpha : \mathcal{W} \to \mathrm{Pic}^4(X)$ is contained in $W \subset \mathrm{Pic}^4(X)$ and induces an isomorphism, $\alpha : \mathcal{W} \xrightarrow{\cong} W$ commuting with the involutions v on domain and image. That is, letting $V := W/\{v\}$, we have the commutative diagram:*

$$\begin{array}{ccc} \mathcal{W} & \xrightarrow{\cong} & W \\ \downarrow & & \downarrow \\ \mathcal{V} & \xrightarrow{\cong} & V \end{array}$$

3.7. Elliptic components and new components. Let X be a ("bi-elliptic") curve defined over $\mathbf{Q}$ satisfying our running hypotheses in this section and let $W := WX$ be—as usual—the Basic Brill–Noether curve attached to X. By an *elliptic involution* of X let us mean an involution $\iota : X \to X$ such that the quotient of X under its action,

$$\mathrm{proj}_\iota : X \to X/\{\sim \iota\} = \mathcal{E},$$

is a curve of genus one. The involution ι induces an action on W and on the constructions of Subsections 3.5 and 3.6. In particular ι commutes with the double cover mapping:

$$\begin{array}{ccc} W & \xrightarrow{\iota} & W \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v} \\ V & \xrightarrow{\iota} & V \end{array}$$

For any such quotient, and any point $u \in \mathcal{E}$ let $j_u : \mathcal{E} \to \mathcal{E}$ denote the canonical (nontrivial) involution fixing the point u, and let

$$\mathrm{proj}_{j_u} : \mathcal{E} \to \mathcal{E}/\{\sim j_u\} =: \mathbf{P}^1_u$$

denote the projection to the (genus zero) quotient (which we denote $\mathbf{P}^1_u$) under the action of j_u. Denote by t_u the running parameter in the projective line $\mathbf{P}^1_u$. For any pair (u, t_u) with $u \in \mathcal{E}$ and $t_u \in \mathbf{P}^1_u$ let $D_\iota(u, t_u) \subset \mathrm{Symm}^4(X)$ be the effective divisor of degree four on X given by

$$D_\iota(u, t_u) := \mathrm{proj}_\iota^{-1} \circ \mathrm{proj}_{j_u}^{-1}(t_u).$$

For each $u \in \mathcal{E}$, then, we have a linear system of divisors of degree four on X parametrized by the variable t_u, giving us a point on W, which we denote $w_\iota(u)$.

The morphism

$$w_\iota : \mathcal{E} \longrightarrow W$$

factors through the quotient $\mathcal{E}'$ of $\mathcal{E}$ under the natural action of the 2-torsion subgroup of its jacobian, i.e., $\mathrm{Pic}^0(\mathcal{E})[2]$. The induced morphism

$$w'_\iota : \mathcal{E}' \hookrightarrow W$$

is a closed immersion, and its image is a (reduced) irreducible component of W defined over the field k. We denote this component $W_\iota \subset W$ and refer to $W_\iota \approx \mathcal{E}'$ as the **k-elliptic component of W associated to** ι. It is fixed by the action of the involution ι on W.

By a **new component** of W we will mean an irreducible component that is not elliptic in the above sense.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

4. Fine Siegel units and fine Siegel points

Let $X := X_1(N)$. A **Fine Siegel unit** on X is a rational function f on X defined over $\bar{\mathbf{Q}}$ whose divisor of zeroes and poles consist only of $\mathbf{Q}$-rational cusps. Let $C(N)$ denote the set of $\mathbf{Q}$-rational cusps; so a fine Siegel unit is a unit in the ring of regular functions on $X_1(N) - C(N)$ (over $\bar{\mathbf{Q}}$). Since the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ preserves the divisor of zeroes-and-poles of a fine Siegel unit, an application of Hilbert's Theorem 90 guarantees that we may normalize our fine Siegel units (by multiplication by an appropriate nonzero scalar) so that they are defined over $\mathbf{Q}$. Such a normalized Siegel unit f is well-defined by its divisor of zeroes-and-poles up to a factor in $\mathbf{Q}^*$ and gives us a $\mathbf{Q}$-rational parametrization $f : X \to \mathbf{P}^1$. Let $\mathcal{Z}(N)$ denote the group of fine Siegel units modulo $\mathbf{Q}^*$. By the Manin–Drinfeld Theorem, $\mathcal{Z}(N)$ is a free abelian group of rank $|C(N)| - 1$. The action of the group Δ of diamond operators on $X_1(N)$ induces an action on $\mathcal{Z}(N)$ and there is a natural metric on $\mathcal{Z}(N)$ given by the geometric degree of the function $f : X_1(N) \to \mathbf{P}^1$. This metric satisfies a triangle inequality:

$$\deg(f \cdot g) \leq \deg(f) + \deg(g),$$

and it scales well, i.e.,

$$\deg(f^n) = |n| \cdot \deg(f)$$

for $n \in \mathbf{Z}$, and is preserved by the action of the diamond operators. See [**Yan09**] for an explicit description of the fine Siegel units in terms of their q-expansions and their expression in relation to specific modular forms.

The following two conditions on $X := X_1(N)$ hold for only a (finite) number of values of N but they do hold for the case $N = 17$.

(1) $X = X_1(N)$ contains no very sporadic points (in the terminology of Section 2) *except for the set of* $\mathbf{Q}$*-rational cusps* $C(N)$.
(2) $\gamma_{\mathcal{C}}(X) < |C(N)|$.

When $N = 17$ these conditions are indeed met[10].

Proposition 4.1. $X_1(17)$ *has no non-cuspidal very sporadic points.*

Proof: There are no non-cuspidal points on $X_1(17)$ of degree 1 by [**Maz77**]; none of degree 2 by [**Kam86**]; and none of degree 3 by [**Par03**].

As we shall see (Proposition 6.7) $X_1(17)$ contains no non-cuspidal sporadic points, as well.

Under hypothesis **(1)** above, every function $\phi : X_1(N) \to \mathbf{P}^1$ of degree $\gamma_{\mathcal{C}}(X)$ and defined over $\mathbf{Q}$ has the property that any of its fibers above points in $\mathbf{P}^1(\mathbf{Q})$ either consists entirely of $\mathbf{Q}$-rational cusps, or contains no $\mathbf{Q}$-rational cusps at all. This is because each fiber is of degree $\gamma_{\mathcal{C}}(X)$ and if it contains a $\mathbf{Q}$-rational cusp, the points of the fiber are all of degree strictly less than $\gamma_{\mathcal{C}}(X)$. That is, these points are all very sporadic, so by **(1)** they are *all* rational cusps. If a fiber of such a ϕ consists entirely of rational cusps, call it a **rational-cuspidal-fiber** of ϕ. By **(2)**, ϕ has at least two rational-cuspidal-fibers. Choosing two rational-cuspidal-fibers of such a $\phi : X \to \mathbf{P}^1$ and composing ϕ with an appropriate linear fractional transformation of $\mathbf{P}^1$ that sends the image of one of those fibers to 0 and the other to ∞ we see that any such ϕ is in the $\mathbf{Q}$-similarity class of a $\mathbf{Q}$-parametrization of $X_1(N)$ by a fine Siegel unit f (of geometric degree equal to the gonality of X).

[10] As has been verified by the first author of this article and Mark van Hoeij, these two conditions are satisfied for $X_1(N)$ for $N = 32$, and for $N < 28$ but not $N = 21$.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

There is a natural way of denoting such a fine Siegel unit f up to the equivalence relation defined by deeming two such Siegel units equivalent if one can be obtained from the other by composition by an appropriate $\mathbf{Q}$-automorphism $b : \mathbf{P}^1 \to \mathbf{P}^1$. Namely, one simply lists the rational-cuspidal-fibers of f giving the divisors with support on cusps that constitutes each of those fibers.

Each divisor with support on the cusps is encoded by $|C(N)|$ integers, where the i-th integer is the multiplicity of the i-th cusp. We display this data for a given f as a matrix, with exactly $|C(N)|$ columns, and as many rows as there are rational-cuspidal-fibers for f. We call it the **rational-cuspidal-fiber matrix** for the $\mathbf{Q}$-linear parametrization class of f.

We also organize these cuspidal-fiber matrices in Δ-orbits. Any such Δ-orbit determines a $\mathbf{Q}$-similarity class of $\mathbf{Q}$-parametrizations of $X_1(N)$ of geometric degree equal to the gonality of X.

Under both hypotheses above, any such f has at least two rational-cuspidal-fibers ($|C(N)| > \gamma_{\mathcal{C}}(X)$ implies that there are at least two fibers containing $\mathbf{Q}$-rational cusps). We can compose f with an appropriate $b : \mathbf{P}^1 \to \mathbf{P}^1$ sending one rational-cuspidal-fiber to 0 and another to ∞, so that $b \circ f$ is a fine Siegel unit.

Consequently

PROPOSITION 4.2. *Under the hypotheses* **(1)** *and* **(2)** *above*

(1) *Any* $\mathbf{Q}$*-parametrization of* $X = X_1(N)$ *of geometric degree* $\gamma_{\mathcal{C}}(X)$ *is represented by at least one fine Siegel unit in* $\mathcal{Z} = \mathcal{Z}(N)$ *of degree* $\gamma_{\mathcal{C}}(X)$*.*
(2) *There are only finitely many classes of* $\mathbf{Q}$*-parametrizations of* $X_1(N)$ *of degree* $\gamma_{\mathcal{C}}(X)$*.*

DEFINITION 4.3. By a **fine Siegel point** on the Basic Brill–Noether variety $WX_1(N)$ let us mean a $\mathbf{Q}$-rational point on $WX_1(N)$ represented by a linear system parametrized by a fine Siegel unit.

COROLLARY 4.4. *Under the hypotheses* **(1)** *and* **(2)** *above, the Basic Brill–Noether variety* $WX_1(N)$ *has only finitely many* $\mathbf{Q}$*-rational points. These are all fine Siegel points and are effectively obtainable.*[11].

The first statement in Corollary 4.4 follows from Proposition 4.2 simply by considering the number of pairs of possible cuspidal-fibers. Effectivity follows because there are effective methods to compute Riemann-Roch spaces of divisors on curves (cf. [**Hes02**]). The computations of cuspidal-fiber matrices can be done for some small values of N (including $N = 17$) by a combination of modular symbol computations implemented by Sage ([**Bos08**, p. 57]) and brute force computations.

When $N = 17$ we shall see that all $\mathbf{Q}$-rational points of $WX_1(N)$ are fine Siegel points. It would be interesting to understand, for more general values of N what portion of $WX_1(N)(\mathbf{Q})$ comes from Siegel (or fine) Siegel points.

A computation of Derickx and van Hoeij [**DvH14**] guarantees that for all $N \leq 40$ there is at least one modular unit of degree equal to the $\mathbf{Q}$-gonality of $X_1(N)$. It follows that if, for these values of N, the $\mathbf{Q}$-gonality were equal to the $\mathcal{C}$-gonality

[11] The same proof gives a similar finiteness and effectivity result for the set of $\mathbf{Q}$-rational points of the Basic Brill–Noether variety WX of *any* curve X defined over $\mathbf{Q}$ that has the property that all its very sporadic points are $\mathbf{Q}$- rational and $|X(\mathbf{Q})|$ is strictly greater than $\gamma_{\mathbf{Q}}(X)$.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

of $X_1(N)$, the corresponding Basic Brill–Noether variety $WX_1(N)$ would contain at least one Siegel point.

5. Digression: 13-torsion

The case of $X = X_1(13)$ is simple, but still instructive, so it may be a good introduction to our discussion of $X_1(17)$. For a study of the arithmetic of $X_1(13)$ and its jacobian, see [**MT73**]. Since $X_1(13)$ is of genus two, it is hyperelliptic; $\gamma_{\mathbf{Q}}(X) = 2$. Let $\sigma : X \to X$ denote the hyperelliptic involution. We thank Andrew Sutherland who communicated to us the following hyperelliptic equation[12] for $X_1(13)$:

$$y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1 := f(x).$$

So, in these coordinates, $\sigma(x, y) = (x, -y)$. The polynomial $f(x)$ is irreducible over the cyclotomic field $\mathbf{Q}(\mu_{13})$ obtained by adjoining all 13-th roots of unity to $\mathbf{Q}$. This guarantees that $J_1(13) := \mathrm{Pic}^0 X_1(13)$ has no nontrivial $\mathbf{Q}(\mu_{13})$-rational 2-torsion, and hence no $\mathbf{Q}$-rational 2-torsion. Let $\mathbf{C} \subset \mathbf{X_1(13)}$ denote the set of six $\mathbf{Q}$-rational cusps. The hyperelliptic involution $\sigma : X_1(13) \to X_1(13)$ preserves the set $\mathbf{C}$, and acts without fixed points on it (the latter statement following immediately from the irreducibility of $f(x)$ over $\mathbf{Q}$). Let

$$\mathbf{C} = \{\mathbf{u}, \sigma\mathbf{u}\} \sqcup \{\mathbf{v}, \sigma\mathbf{v}\} \sqcup \{\mathbf{w}, \sigma\mathbf{w}\}$$

be the orbit decomposition of $\mathbf{C}$ under the action of σ.

We have the natural projection,

$$\eta_2 : \mathrm{Sym}^2(X) \longrightarrow \mathrm{Pic}^2(X), \tag{5.1}$$

with the basic Brill–Noether variety $W = W(X) \subset \mathrm{Pic}^2(X)$ equal to a single point—call it $0 \in Pic^2(X)$. It can be taken to be the image of any of the three $\mathbf{Q}$-rational points

$$(u, \sigma u), (v, \sigma v), (w, \sigma w) \ \in \ \mathrm{Sym}^2(X).$$

This allows us to make the natural identification, rational over $\mathbf{Q}$, $\mathrm{Pic}^0(X) \cong \mathrm{Pic}^2(X)$, sending 0 to 0, and to view $\mathrm{Pic}^2(X)$ in a canonical way as an abelian surface over $\mathbf{Q}$. By [**MT73**] the Mordell–Weil group of $\mathrm{Pic}^2(X)$ is of order 19.

The morphism η_2 is an isomorphism on the inverse image of the complement of the origin $\{0\}$ in $\mathrm{Pic}^2(X)$ and identifies $\mathrm{Sym}^2(X)$ as the blow-up of $\mathrm{Pic}^2(X)$ at the point 0. Let

$$\mathcal{G} \subset \mathrm{Sym}^2(X)$$

denote this exceptional divisor. We may view, then, $\mathcal{G} := \eta_2^{-1}(0)$ as the locus $\{(x, \sigma x) \mid x \ \in X\}$, or more properly as the quotient X/σ of X under the action of the involution σ. In terms of the parameters (x, y) above, we may say that $\mathcal{G}$ is parametrized by the variable x.

We also interpret this as saying that there is a unique one-parameter family of elliptic curves over quadratic number fields containing (correspondingly rational) 13-torsion, this family being rationally parameterized by $\mathcal{G}$.

We focus, now, on the isomorphism over $\mathbf{Q}$:

$$\eta_2 : \mathrm{Sym}^{2,\#}(X) = \mathrm{Sym}^2(X) - \mathcal{G} \quad \xrightarrow{\cong} \quad \mathrm{Pic}^2(X) - \{0\}. \tag{5.2}$$

[12]Such an equation had also been computed by J. Blass and was shown to be irreducible over Q; see the reference [1] in [**MT73**].

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

THEOREM 5.1. *The morphism η_2 induces a one-one correspondence between these two finite sets of cardinality* 18*:*

- $\mathrm{Sym}^2(\mathcal{C}) - \{(u, \sigma u), (v, \sigma v), (w, \sigma w)\}$
- *The set of* $\mathbf{Q}$*-rational points of* $\mathrm{Pic}^2(X) - \{0\}$.

Proof: From the above discussion, it follows that η_2 is an injection of the set $\mathrm{Sym}^2(\mathcal{C}) - \{(u, \sigma u), (v, \sigma v), (w, \sigma w)\}$ into $\mathrm{Pic}^2(X) - \{0\}$. The theorem follows by computing the cardinality of the two sets in question; i.e.,

$$\binom{6}{2} + 6 - 3 \quad = \quad 19 - 1.$$

COROLLARY 5.2. *Every sporadic point for $X_1(13)/\mathbf{Q}$ is cuspidal. Elliptic curves defined over quadratic fields possessing (correspondingly rational)* 13*-torsion are parametrized by the non-cuspidal* $\mathbf{Q}$*-rational points of $\mathcal{G} = \mathbf{P}^1$ via the natural hyperelliptic projection $X_1(13) \to \mathcal{G}$.*

6. Families of 17-torsion

The curve $X = X_1(17)$ is of genus 5 with $\mathbf{Q}$-gonality and $\mathbf{C}$-gonality both equal to 4. The basic Brill–Noether variety $WX_1(17)$ is a curve.

The curve $X_1(17)$ has no non-cuspidal very sporadic points (Proposition 4.1) and no non-cuspidal sporadic points (Proposition 6.7). Andrew Sutherland has computed elegant equations for these modular curves in [**Sut**]. The equation for $X_1(17)$ is particularly crisp[13]:

There is a birational morphism (over $\mathbf{Q}$) of $X_1(17)$ onto the bi-projective curve of bi-degree $(4, 4)$ in $\mathbf{P}^1 \times \mathbf{P}^1$ cut out by the polynomial

$$(*) \quad x^4y - x^3y^3 - x^3y + x^2y^4 + x^2y - x^2 - xy^4 + xy^3 - xy^2 + xy + y^3 - 2y^2 + y = 0.$$

This morphism is an embedding when restricted to the complement of the cusps, $Y_1(17) \subset X_1(17)$ into $\mathbf{P}^1 \times \mathbf{P}^1$. Projection to the first factor is given by the modular unit[14] $x := E_5E_6/E_1E_3$ and the projection to the second factor is given by the modular unit $y := E_6E_7/E_2E_8$. Both x and y are functions of degree 4 and in fact there is another function of degree 4, namely:

$$z = \frac{y(x^2 - yx + y - 1)}{(y-1)^2 x}.$$

An example of the type of result that we prove (based, of course, on the results already mentioned) is the following:

THEOREM 6.1. *Any elliptic curve defined over a field of degree ≤ 4 possessing points of order* 17 *defined over that field can be obtained by applying a diamond operator to a point of $X_1(17)$ for which one of the functions x, y takes on a rational value $\neq 0, 1$ or z takes a value $\neq 0$. Conversely, setting x, y to a rational value $\neq 0, 1$ or z to a value $\neq 0$ defines an elliptic curve over a field of degree four with a rational* 17*-torsion point.*

[13] As we understand it, this equation was originally written down by Cady and Elkies; see also a closely related description of $X_1(17)$ in [**JKL11b**].

[14] Here we are using the notation of Yang [**Yan09**], following Kubert-Lang [**KL81**].

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

Moreover, the rational parameters x, y, z give, up to $\mathbf{Q}$*-similarity*[15] *all* $\mathbf{Q}$*-rational parametrizations of $X_1(17)$ of degree equal to its gonality (i.e., degree $= 4$). The Galois group of the finite extension*

$$\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$$

is the full symmetric group[16] *S_4 while the finite mappings*

$$y, z : X_1(17) \to \mathbf{P}^1$$

factor through the bi-elliptic representation

$$X_1(17) \longrightarrow X_1(17)/\{\text{action of } \langle 13\rangle\} = X_1(17)/\{\text{action of } \langle 3\rangle^4\}$$

and their Galois group is the dihedral group D_4.

The functions x, y, z of the theorem are in the equivalence classes of $\mathbf{Q}$-parametrizations of type $(\mathbf{C}), (\mathbf{A}), (\mathbf{B})$ described in subsection 6.2 below.

The fun here is that there are, in fact, two distinct ways of getting at the diophantine problem involved, as discussed above. They dovetail in a nice way. We can approach the problem either by considering:

- $\mathbf{Q}$-rational points on the Basic Brill–Noether modular curve WX,

or

- rational cuspidal divisors and "fine" Siegel units.

6.1. Via the Basic Brill–Noether modular curve. We have computed the Basic Brill–Noether modular curve $W := WX_1(17)$ to be a double cover of a plane quintic (reducible) curve

$$(*) \qquad V: \quad X \cdot (X^4 - 3X^2Y^2 - 3X^2Z^2 + Y^4 + 2Y^3Z + 3Y^2Z^2 - 2YZ^3 + Z^4) = 0.$$

The involution v of W that is the automorphism of the double cover $W \to V$ (the identity on V) has three descriptions. First, it is given by the diamond operator involution $\langle 13\rangle = \langle 3\rangle^4$. Secondly, it is also the involution induced on W (via the Serre duality theorem) from the transformation of divisors of degree four $D \mapsto K - D$ where K is the canonical divisor (of degree 8) on $X_1(17)$. The third description comes from what one might call the *canonical representation* of $W \to V$ as described in some generality in Subsections 3.5 and 3.6 above.

The group, Δ, of $\mathbf{Q}$-automorphisms of X is canonically isomorphic to $(\mathbf{Z}/17\mathbf{Z})^*/\{\pm 1\}$. The operator $\langle 3\rangle \in \Delta$ is a generator.

Let $S_k := S_k(\Gamma_1(17))$ denote the $\mathbf{Q}$-vector space of cuspforms of weight k on $\Gamma_1(17))$. Since the genus of $X_1(17)$ is 5 we have $\dim S_2 = 5$. The characteristic polynomial of $\langle 3\rangle$ acting on S_2 is $(x-1)(x^4+1)$, this means that there is a basis $\omega_0, \ldots, \omega_4 \in S_2$ such that with respect to this basis we have:

$$\langle 3\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

[15] Recall the definition in Proposition 3.1: two parametrizations are **Q-similar** if one can be brought to the other by composition with appropriate $\mathbf{Q}$-isomorphisms of domain and range.

[16] Hilbert's Irreducibility theorem would then guarantee infinitely many specializations $x \mapsto a \in \mathbf{Q}^*$ give a quartic polynomial in $\mathbf{Q}[y]$ with full symmetric Galois group.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

One such basis is given by

$$\omega_0 := q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 + O(q^9) \tag{6.1}$$

$$\omega_1 := q - q^2 - q^3 + q^6 - q^7 + q^8 + O(q^9) \tag{6.2}$$

$$\omega_2 := q^2 - q^3 - 2q^4 + q^5 + q^6 + q^7 + O(q^9) \tag{6.3}$$

$$\omega_3 := -q^2 + q^3 + q^4 + q^5 - q^6 - q^7 - q^8 + O(q^9) \tag{6.4}$$

$$\omega_4 := q^3 - 2q^4 + q^6 - q^7 + 3q^8 + O(q^9) \tag{6.5}$$

Every nonzero element in $\mathrm{Sym}^2(S_2)$ defines a quadratic form in the ω_i and and hence a quadric in $\mathbf{P}^4$. Now let $Y \subseteq \mathrm{Sym}^2(S_2)$ be the kernel of the natural map:

$$\mathrm{Sym}^2(S_2) \to S_4$$

Then Y will be a 3-dimensional space with basis e_0, e_1, e_2 given by

$$e_0 := \omega_0^2 - \omega_1^2 - \omega_2^2 - \omega_3^2 - \omega_4^2 \tag{6.6}$$

$$e_1 := 2\omega_1\omega_2 + 2\omega_1\omega_3 - 2\omega_3\omega_4 \tag{6.7}$$

$$e_2 := 2\omega_2\omega_3 + 2\omega_1\omega_4 + 2\omega_2\omega_4 \tag{6.8}$$

The matrix of $\langle 3 \rangle$ acting on Y with respect to this basis is:

$$\langle 3 \rangle = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

Let (a_0, a_1, a_2) be coordinates of Y with respect to the basis e_0, e_1, e_2. Now consider the locus $V \subset \mathbf{P}^2 = \mathbf{P}(Y)$ corresponding to the singular quadrics in $\mathbf{P}^4$. This locus will be given by the single homogenous equation of degree 5, **(*)** above.

Each of these singular quadrics has (generally) two rulings by planes, and each of these planes intersect the canonically embedded curve X in an (effective, of course) divisor of degree 4. Each ruling, then, gives a unique linear system of effective divisors of degree 4 on X. That is, we can identify the Basic Brill–Noether curve W with the locus of rulings on these singular quadrics. The involution v simply switches rulings on the same singular quadric.

The plane quintic V breaks up into the union of a line

$$V_0 : \quad X = 0$$

and a plane quartic

$$V_1 : \quad X^4 - 3X^2Y^2 - 3X^2Z^2 + Y^4 + 2Y^3Z + 3Y^2Z^2 - 2YZ^3 + Z^4 = 0$$

and $W = W_0 \cup W_1$ is a union of two irreducible components where W_0 (a double cover of V_0) is an elliptic curve of Cremona type 17a4.

The curve of genus one, W_0 is directly related to the bi-elliptic representation of $X_1(17)$. It has four rational points, two of which yield parameterizations in the $\mathbf{Q}$-similarity class of the function y and the other two yield parameterizations in the class of z.

The more interesting component W_1 is given (birationally) as a double cover of V_1 given by extracting a "square root" of the function

$$(2Y^2Z + 2XY^2 + XZ^2 - X^3)/X^3$$

on V_1.

Much of the internal structure of the Basic Brill–Noether curve W is directly related to the bi-elliptic representation of $X_1(17)$ mentioned above, so let us return

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

to it with a bit more detail. The diamond operators of $X_1(17)$ acting functorially on W preserve the irreducible component W_1 and we have the following curiously similar sequences of double covers:

- Consider the sequence of double covers:[17]

$$\begin{array}{ccccc} X & \longrightarrow & X/(\langle 3\rangle^4) & \longrightarrow & X/(\langle 3\rangle^2) & \longrightarrow & X/(\langle 3\rangle) \\ & & \downarrow \approx & & \downarrow \approx & & \downarrow = \\ & & 17a4 & \longrightarrow & 17a2 & \longrightarrow & X_0(17) \end{array}$$

  We easily compute that $X/(\langle 3\rangle^4), X/(\langle 3\rangle^2)$ and $X/(\langle 3\rangle)$ are curves of genus 1, and the automorphism $\langle 3\rangle$ acts freely on them of order $4, 2$ and 1 respectively. In particular, the action of $\langle 3\rangle$ on $X/(\langle 3\rangle^4)$ can be understood as the action of translation by a ($\mathbf{Q}$-rational) point $\mathcal{P}$ of order 4 in the jacobian, $\mathcal{J} := \mathrm{Pic}^0(X/(\langle 3\rangle^4)))$. This pins things down, after consulting Cremona's tables, forcing (the jacobian of) $X/(\langle 3\rangle^4)$ to be $17a4$ (which is the only curve of conductor 17 that has a rational 4-torsion point, the quotient by which is isomorphic to $X_0(17)$) and forcing (the jacobian of) $X/(\langle 3\rangle^2)$ to then be 17a2.

  It is an exercise to see, with no computation at all, that W_0 can be canonically identified as the curve of genus one given as the quotient of the curve $X/(\langle 3\rangle^4)$ by the natural action of the 2-torsion subgroup of its jacobian. It follows then that W_0 is isomorphic to 17a4, and therefore has exactly four rational points. These four points break up into two orbits under the action of the 'diamond operators' Δ contributing to two $\mathbf{Q}$-similarity classes represented by the functions "y" and "z" of our theorem.
- The curve W_1 is a curve of genus 7, but is also directly related to 17a4 and neatly mimics the sequence displayed in the previous bullet as follows. Consider the diamond operators acting on W_1 which can be computed to produce the sequence of double covers:

$$\begin{array}{ccccccccc} W_1 & \longrightarrow & W_1/(\langle 3\rangle^4) & \longrightarrow & W_1/(\langle 3\rangle^2) & \longrightarrow & W_1/(\langle 3\rangle) & \longrightarrow & X_0(17) \\ & & \downarrow = & & \downarrow \approx & & \downarrow \approx & & \downarrow = \\ & & V_1 & \longrightarrow & 17a4 & \longrightarrow & 17a2 & \longrightarrow & X_0(17) \end{array}$$

The curve V_1 has exactly four $\mathbf{Q}$-rational points: $(1, \pm 1, \pm 1)$ and the eight points in W_1 comprising the inverse image of those four points are all $\mathbf{Q}$-rational, and therefore give the full set of $\mathbf{Q}$-rational points of W_1. These eight point comprise a single Δ-orbit. Therefore they give rise to a unique $\mathbf{Q}$-similarity class of rational parametrizations of $X_1(17)$, for which the function "x" of the theorem is a representative.

6.2. Via Fine Siegel Units. As is clear from the account already given, to compute the rational points on the Basic Brill–Noether curve $WX_1(17)$ is not greatly difficult since each of its connected components is a perfectly specified finite

[17] We use Cremona's classification to refer to some of the elliptic curves that occur in these computations.

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

cover of an elliptic curve possessing only four rational points. Section 4 above offers an utterly independent way of making this computation: by Proposition 4.1 the only very sporadic points on $X_1(17)$ are the eight rational cusps, and therefore any $\mathbf{Q}$-rational function ϕ of degree 4 on $X_1(17)$ has the curious property, as discussed in section 4 that

- any of its fibers that contain even a single rational cusp must consist entirely of rational cusps—call such a fiber a **rational cuspidal fiber** and
- there are at least two such rational cuspidal fibers.

It follows that by composing ϕ with an appropriate $\mathbf{Q}$-automorphism of $\mathbf{P}^1$ one gets a fine Siegel unit. It follows that the problem of computing the $\mathbf{Q}$-rational points on $WX_1(17)$ is essentially equivalent to that of computing fine Siegel units of degree four. As mentioned in Section 4, this is a finite computation.

We will be giving the collection of all fine Siegel units f of geometric degree 4—up to composition by appropriate $\mathbf{Q}$-automorphisms $b : \mathbf{P}^1 \to \mathbf{P}^1$. This we do by listing the divisors that describe the cuspidal-fibers for each f and organizing these cuspidal-fiber matrices in Δ-orbits. Each such Δ-orbit describes *one* class of $\mathbf{Q}$-parametrizations of $X_1(17)$ (of geometric degree 4); there are three of them.

Each divisor with support on these rational cusps is encoded by 8 integers, where the i-th integer is the multiplicity of the i-th cusp in the ordering:

$$\{2/17, 3/17, 4/17, 5/17, 6/17, 7/17, 8/17, \infty\}.$$

We display this data for a given f as a matrix, with exactly 8 columns, and as many rows as there are cuspidal-fibers for f. This is the **cuspidal-fiber matrix of** f as discussed in section 4 above.

The first two classes factor through the quotient of $X_1(17)$ under the action of the involution $\langle 13\rangle$. That is, they factor through the double cover

$$X_1(17) \quad \xrightarrow{\pi} \quad X_1(17)/\langle 13\rangle.$$

The quotient curve $X_1(17)/\langle 13\rangle$ is isomorphic over $\mathbf{Q}$ to the elliptic curve $E := 17A4$ in Cremona's classification. The Mordell–Weil group of 17A4 (over $\mathbf{Q}$), is cyclic of order four. Make one (of the four possible) identifications—rational over $\mathbf{Q}$:

$$X_1(17)/\langle 13\rangle \quad \overset{\iota}{\cong} \quad E$$

The determination of the cuspidal-fiber matrix for each of these two classes uses a minimum of computation; i.e., we work essentially by 'pure thought,' given the fact that $E(\mathbf{Q})$ is cyclic of order four. Since there are eight rational cusps on $X_1(17)$ and $\iota \cdot \pi$ is of degree two, these eight rational cusps are unramified for the mapping $\iota \cdot \pi$, and the set of them map surjectively—by a two-to-one mapping—to $E(\mathbf{Q})$. Now E itself has precisely four $\mathbf{Q}$-rational involutions υ_a such that $E/\langle \upsilon_a\rangle \cong \mathbf{P}^1$. These are given by the formulae $x \mapsto a - x$ for $a \in E(\mathbf{Q})$. Note that

- $|E(\mathbf{Q})/\langle \upsilon_a\rangle| = 3$ if a is trivial or of order two, while
- $|E(\mathbf{Q})/\langle \upsilon_a\rangle| = 2$ if a is one of the two generators of $E(\mathbf{Q})$.

Denote

$$f_a : E \to E/\langle \upsilon_a\rangle \approx \mathbf{P}^1$$

the double cover associated to the involution υ_a. Now if t_b is translation by b with b a point of order 4 and if $a' - a$ is in $E(\mathbf{Q})[2] \setminus \{0\}$ then $\upsilon_a = t_b \circ \upsilon_{a'} \circ t_b^{-1}$, implying

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

that f_a and $f_{a'}$ are in the same parameterization class. So we have (at most) two $\mathbf{Q}$-rational classes of parametrizations of E of degree two coming from the four maps f_a.That these are in fact different equivalence classes can be seen from the bullets above. For more specificity, choose an identification ("$\approx$") of $E/\langle \upsilon_a \rangle$ with $\mathbf{P}^1$ so that in the first case above $E(\mathbf{Q})/\langle \upsilon_a \rangle$ is identified with the set $\{0, 1, \infty\}$ (any order will do) and in the second case it is identified with $\{0, \infty\}$. Fixing such an identification, but composing with $\iota \cdot \pi$ for the four possible choices of ι gives two Δ-orbits of fine Siegel units of degree four on $X_1(17)$.

The cuspidal-fiber matrices for the two $\mathbf{Q}$-parametrizations of $X_1(17)$ (of geometric degree 4) that factor through $X_1(17)/\langle 13 \rangle$ are immediately computable from this discussion. In particular they each consist of a single Δ-orbit of order two. We'll call them "$\mathbf{Q}$-similarity classes **(A)** and **(B)**."

- **Q-similarity class of parametrizations (A):**

$$M_1 := \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

$$M_2 := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \end{pmatrix}$$

- **Q-similarity class of parametrizations (B):**

$$M_3 := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_4 := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Far less evident is the third (and last) class of $\mathbf{Q}$-parametrization of $X_1(17)$ of degree four. This class ("**(C)**") is given (as shown in the discussion below) by a single Δ-orbit of order eight, described by eight cuspidal-fiber matrices $M_5, M_6, \ldots, M_{12}$ permuted by the action of Δ. These 8 matrices correspond to the 8 rational points of W_1.

- **Q-similarity class of parametrizations (C):**

$$M_5 := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$M_6 := \langle 3 \rangle M_5 \quad \cdots \quad M_{12} := \langle 3 \rangle^7 M_5$$

Depending on how you decide which of the three rational cuspidal fibers will be *zeroes* of your function and which *poles* you get different $\mathbf{Q}$-linear parameterizations of $X_1(17)$ and different fine Siegel units. For example E_1E_3/E_5E_6 has the first row of M_5 as zero-divisor and the second row as polar-divisor, while $E_3E_4E_8/E_2E_6E_7$ has the third row of M_5 as zero-divisor and the second row as polar-divisor.

We can summarize as follows. Let

$$\Gamma \subset X_1(17)(\bar{\mathbf{Q}})$$

denote the set of non-cuspidal algebraic points of $X_1(17)$ defined over number fields of degree four. If $\gamma \in \Gamma$ let $\mathbf{Q}(\gamma)$ denote the number field (of degree four) over which γ is defined. Say that γ is of type **(A)**, **(B)** respectively **(C)** if the projection of γ

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

under one of the $\mathbf{Q}$-parametrization in the equivalence class **(A)**, **(B)** respectively **(C)** is a $\mathbf{Q}$-rational point of $\mathbf{P}^1$. Let $\Gamma_{(\mathbf{A})} \subset \Gamma$ denote the subset of points of type **(A)**; and similarly for $\Gamma_{(\mathbf{B})}$ and $\Gamma_{(\mathbf{C})}$.

THEOREM 6.2. *The set Γ (of non-cuspidal algebraic points of $X_1(17)$ defined over number fields of degree four) is the disjoint union*

$$\Gamma \quad = \quad \Gamma_{(\mathbf{A})} \bigsqcup \Gamma_{(\mathbf{B})} \bigsqcup \Gamma_{(\mathbf{C})}.$$

PROOF. The above discussion gives us the full list of $\mathbf{Q}$-similar classes of $\mathbf{Q}$-parametrized points of degree 4 on $X_1(17)$. The fact that $W_4^2 X_1(17)$ is empty (because $X_1(17)$ has no functions of degree 3) shows that the union above is a *disjoint union*. It remains to show that $X_1(17)$ has no very sporadic, or sporadic points that are not cusps. For this, see section 6.3 below. □

PROPOSITION 6.3. *Let x, y, z be the functions from theorem* 6.1*, then the Galois groups of $\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$, $\mathbf{Q}(y) \subset \mathbf{Q}(X_1(17))$ and $\mathbf{Q}(z) \subset \mathbf{Q}(X_1(17))$ are S_4, D_4 and D_4 respectively.*

PROOF. Let K_x denote the Galois closure of $\mathbf{Q}(x) \subset \mathbf{Q}(X_1(17))$, then by looking at matrix M_5 one sees that $[K_x : \mathbf{Q}(X_1(17))]$ has to be divisible by 6, implying that 24 divides $[K_x : \mathbf{Q}(x)]$ hence the Galois group has to be S_4.

For the proof that the other two Galois groups are D_4, one can use the following observation: Suppose that $M \subset L \subset K$ is a tower of field extensions with $[L : M] = [K : L] = 2$ and K/M is not Galois, then K/M has Galois group D_4. One can then apply this observation to $\mathbf{Q}(y) \subset \mathbf{Q}(X_1(17)/\langle 3^4 \rangle) \subset \mathbf{Q}(X_1(17))$ and $\mathbf{Q}(z) \subset \mathbf{Q}(X_1(17)/\langle 3^4 \rangle) \subset \mathbf{Q}(X_1(17))$. Now $\mathbf{Q}(X_1(17))/\mathbf{Q}(y)$ and $\mathbf{Q}(X_1(17))/\mathbf{Q}(z)$ are not Galois follows from the fact that there is no subgroup $H \subset \mathrm{Aut}_{\mathbf{Q}}(X_1(17)) = (\mathbf{Z}/17\mathbf{Z})^*/\pm 1$ of order 4 such that $X_1(17)/H \cong \mathbf{P}^1$.

□

6.3. Sporadic and very sporadic points on $X_1(17)$. The computations in the previous section show that the number of g_4^1's on $X_1(17)$ that are defined over $\mathbf{Q}$ is exactly 12. This is actually proved twice, once by proving $12 = 4 + 8 = \#W_0(\mathbf{Q}) + \#W_1(\mathbf{Q})$, and once by using proposition 4.2 and computing that there are exactly 12 cuspidal fiber matrices corresponding to fine Siegel units of degree 4. The main goal of this section is to prove the following theorem:

THEOREM 6.4. *Every point on $X_1(17)$ of degree 4 over $\mathbf{Q}$ is in one of the 12 g_4^1's.*

For the proof of this theorem we will use a slight modification of a theorem due to Michael Stoll in [**Kam89**].

Let $C/\mathbf{Q}$ be a curve with jacobian J, and let $d \geq 1$ be an integer. Let C^d be the dth power, and $C_d := \mathrm{Symm}^d(C)$ the dth symmetric power of C. Let

$$C_d^{\{1\}} := C_d \times_J W_d^1(C).$$

So $C_d^{\{1\}} \subset C_d$ is the closed subvariety parametrizing those divisors D of degree d such that $\dim H^0(O_C(D), C) - 1 = \dim |D| \geq 1$.

Denote by $s : C^d \to C_d$ the natural quotient map.

THEOREM 6.5. *Let ℓ be a prime of good reduction for C. Let $P_0 \in C(\mathbf{Q})$ be chosen as base-point for an embedding $\iota : C \to J$. This also induces morphisms*

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

$C^d \to C_d \to J$. *If the following assumptions hold:*

(1) $\ell > 2$ *or* $J(\mathbf{Q})[2]$ *injects into* $J(\mathbf{F}_\ell)$ *(for example,* $\#J(\mathbf{Q})$ *is odd).*
(2) $J(\mathbf{Q})$ *is finite.*
(3) *The reduction map* $C(\mathbf{Q}) \to C(\mathbf{F}_\ell)$ *is surjective.*
(4) *The intersection of the image of* $C_d(\mathbf{F}_\ell)$ *in* $J(\mathbf{F}_\ell)$ *with the image of* $J(\mathbf{Q})$ *under reduction mod* ℓ *is contained in the image of* $C^d(\mathbf{F}_\ell)$.

Then $C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q})$ *is contained in the image of* $C^d(\mathbf{Q}) \to C_d(\mathbf{Q})$.

PROOF. Let ρ_X denote the reduction map $X(\mathbf{Q}) \to X(\mathbf{F}_\ell)$, where X is a smooth projective variety over $\mathbf{Q}$ with good reduction at ℓ.

From assumptions (2) and (1) we can deduce that $\rho_J : J(\mathbf{Q}) \to J(\mathbf{F}_\ell)$ is injective. By the definition of $C_d^{\{1\}}$ it is also clear that $C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) \to J(\mathbf{Q})$ is injective.

Finally (3) shows that $\rho_C^d : C^d(\mathbf{Q}) \to C^d(\mathbf{F}_\ell)$ is surjective.

$$\begin{array}{ccccc}
 & & C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) & & \\
 & & \downarrow & \overset{\iota}{\searrow} & \\
C^d(\mathbf{Q}) & \xrightarrow{s} & C_d(\mathbf{Q}) & \xrightarrow{\iota} & J(\mathbf{Q}) \\
\downarrow{\scriptstyle \rho_{C^d}} & (3) & \downarrow{\scriptstyle \rho_{C_d}} & (2,1) & \downarrow{\scriptstyle \rho_J} \\
C^d(\mathbf{F}_\ell) & \xrightarrow{s} & C_d(\mathbf{F}_\ell) & \xrightarrow{\iota} & J(\mathbf{F}_\ell).
\end{array}$$

Now let $P \in C_d(\mathbf{Q}) \setminus C_d^{\{1\}}(\mathbf{Q}) \to J(\mathbf{Q})$. We want to show that there is a $Q \in C^d(Q)$ such that $s(Q) = P$. Now $\rho_J \circ \iota(P) = \iota \circ \rho_{C_d}(P) \in J(\mathbf{F}_\ell)$ so from assumption (4) it follows that there is a $\overline{Q} \in C^d(\mathbf{F}_\ell)$ such that $\iota \circ s(\overline{Q}) = \rho_J \circ \iota(P)$. Let $Q \in C^d(\mathbf{Q})$ be such that $\rho_{C^d}(Q) = \overline{Q}$ then

$$\rho_J \circ \iota \circ s(Q) = \iota \circ s(\overline{Q}) = \rho_J \circ \iota(P).$$

The injectivity of ρ_J implies $\iota \circ s(Q) = \iota(P)$ and because $P \notin C_d^1(\mathbf{Q})$ we know that $s(Q) = P$. □

COROLLARY 6.6. *If the above hypotheses hold for* $d = \gamma_{\mathcal{C}}(C)$ *then all sporadic points of* C *are* $\mathbf{Q}$*-rational.*

PROPOSITION 6.7. *There are no sporadic non-cuspidal points on* $X_1(17)$.

PROOF. We apply Theorem 6.5 taking $C := X = X_1(17)$. We take $\ell = 3$, so (1) holds. Since $J_1(17)(\mathbf{Q})$ is of finite order[18], condition (2) holds. The Hasse-Weil bound implies that for an elliptic curve E over $\mathbf{F}_3$ we have $\#E(\mathbf{F}_3) \leq 3+1+2\sqrt{3} < 8$ so this E cannot have an $\mathbf{F}_3$-rational point of order 17 showing that $X = X_1(17)(\mathbf{F}_3)$ consists entirely of cusps, which gives (3). Finally we verified with a computation in magma that assumption (4) is also satisfied.

□

[18] $J_1(17)(\mathbf{Q})$ is of order $584 = 8 \cdot 73$ ([**Kam85**] for the prime-to-2 part; and for the 2-torsion: [**Par03**]). Regarding values of N for which $J_1(N)(\mathbf{Q})$ is finite, consult Prop. 6.2.1 in [**CES03**].

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

7. Appendix: Gonality

If X is a curve over k the k-**gonality** of X is the smallest positive integer $\gamma = \gamma_k(X)$ for which there is a degree γ mapping $f : X \to \mathbf{P}^1$ defined over k, or–equivalently–a k-parametrization of X of degree γ.

LEMMA 7.1. *Let k be algebraically closed. The k-gonality $\gamma = \gamma_k(X)$ is the smallest integer d for which equivalently:*

- *there exists a positive dimensional linear system of effective divisors of degree d on X defined over k;*
- *$W^1_d(X)$ is nonempty. (Here $W^r_d(X)$ denotes the Brill–Noether variety that classifies g^r_d's on X.)*

PROOF. The equivalence of the two bullets above follows from the definition of $W^1_d(X)$ and the assumption that k is algebraically closed. Suppose given a positive dimensional linear system of effective divisors of degree d on X defined over k, and suppose that d is the smallest degree for which there exists such a linear system. Let $D \subset X \times \mathbf{P}^1$ be the (effective) Cartier divisor—which we may assume to be a reduced and irreducible curve in $X \times \mathbf{P}^1$—representing the linear system so that if $\pi_{\mathbf{P}^1}$ and π_X denote projection to the indicated factors, then

- $\pi_{\mathbf{P}^1} : D \to \mathbf{P}^1$ is finite flat of degree d, and
- $\pi_X \circ \pi^{-1}_{\mathbf{P}^1} : t \mapsto D_t$ gives the linear system, with t a parameter of $\mathbf{P}^1$.

Clearly $d \leq \gamma$. Our task is to find a degree d mapping $f : X \to \mathbf{P}^1$ defined over k, proving that $\gamma \leq d$. We will show that for $t_1 \neq t_2 \in \mathbf{P}^1(k)$ the support of D_{t_1} is disjoint from that of D_{t_2}. Suppose it was not. Then write $D_{t_i} = \Delta + \Delta_i$ for $i = 1, 2$, where Δ consists of an effective divisor of positive degree common to both D_{t_1} and D_{t_2}. We have that Δ_i are effective divisors, $\Delta_1 \neq \Delta_2$ and yet $\Delta_1 \equiv \Delta_2$. But this would give us a positive dimensional linear system of degree strictly less than d, contrary to assumption.

Therefore: **(*):** the support of the divisors D_t are disjoint for distinct values of t.

Now view D as an algebraic system of divisors on $\mathbf{P}^1$ parametrized by X. That is, form the correspondence $D^x := \pi_{\mathbf{P}^1} \circ \pi_X^{-1}(x)$ for $x \in X$. By **(*)** the support of each fiber D_x consists of a single point. Since D is reduced, the projection $\pi_X : D \to X$ is an isomorphism. Define $f := \pi_{\mathbf{P}^1} \circ \pi_X^{-1} : X \to \mathbf{P}^1$. □

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20** (1996), 1005–1011, DOI 10.1155/S1073792896000621. MR1422373

[AH91] Dan Abramovich and Joe Harris, *Abelian varieties and curves in $W_d(C)$*, Compositio Math. **78** (1991), no. 2, 227–238. MR1104789

[Bos08] J. Bosman, Explicit computations with modular Galois representations, PhD Thesis, 2008 `http://hdl.handle.net/1887/13364`.

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985. MR770932

[ACG11] Enrico Arbarello, Maurizio Cornalba, and Pillip A. Griffiths, *Geometry of algebraic curves. Volume II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 268, Springer, Heidelberg, 2011. With a contribution by Joseph Daniel Harris. MR2807457

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

[CCS13] Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), no. 2, 447–479, DOI 10.1142/S1793042112501436. MR3005559

[DvH14] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71, DOI 10.1016/j.jalgebra.2014.06.026. MR3244637

[Kam89] S. Kamienny, *Torsion points on elliptic curves over fields of low degree*, Manuscripta Math. **65** (1989), no. 3, 349–355, DOI 10.1007/BF01303042. MR1015660

[Dol12] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view. MR2964027

[CES03] Brian Conrad, Bas Edixhoven, and William Stein, *$J_1(p)$ has connected fibers*, Doc. Math. **8** (2003), 331–408. MR2029169

[Fal94] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83, DOI 10.1007/BF02758637. MR1264340

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445, DOI 10.1006/jsco.2001.0513. MR1890579

[Hoe14] M. Hoeij, Low degree places on the modular curve $X_1(N)$ (preprint `http://arxiv.org/abs/1202.4355`)

[JKL11a] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 273, 579–591, DOI 10.1090/S0025-5718-10-02369-0. MR2728995

[JKL11b] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 276, 2395–2410, DOI 10.1090/S0025-5718-2011-02493-2. MR2813367

[Kam82] S. Kamienny, *On $J_1(p)$ and the conjecture of Birch and Swinnerton-Dyer*, Duke Math. J. **49** (1982), no. 2, 329–340. MR659944

[Kam85] S. Kamienny, *Rational points on modular curves and abelian varieties*, J. Reine Angew. Math. **359** (1985), 174–187, DOI 10.1515/crll.1985.359.174. MR794803

[Kam86] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162, DOI 10.1215/S0012-7094-86-05310-X. MR835802

[Kam92a] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689

[Kam92b] S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices **6** (1992), 129–133, DOI 10.1155/S107379289200014X. MR1167117

[KM95] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque **228** (1995), 3, 81–100. With an appendix by A. Granville; Columbia University Number Theory Seminar (New York, 1992). MR1330929

[KN12] Sheldon Kamienny and Filip Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), no. 3, 291–305, DOI 10.4064/aa152-3-5. MR2885789

[KM88] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. MR931956

[KL81] Daniel S. Kubert and Serge Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York-Berlin, 1981. MR648603

[LL85] Michael Laska and Martin Lorenz, *Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$*, J. Reine Angew. Math. **355** (1985), 163–172, DOI 10.1515/crll.1985.355.163. MR772489

[LR13] Álvaro Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305, DOI 10.1007/s00208-013-0906-5. MR3084348

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230

Licensed to AMS.
License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms

[MT73] B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49, DOI 10.1007/BF01425572. MR0347826

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (French), Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059. MR1369424

[Mom84] Fumiyuki Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **96** (1984), 139–165. MR771075

[Naj16] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett. **23** (2016), no. 1, 245–272, DOI 10.4310/MRL.2016.v23.n1.a12. MR3512885

[Par03] Pierre Parent, *No 17-torsion on elliptic curves over cubic number fields* (English, with English and French summaries), J. Théor. Nombres Bordeaux **15** (2003), no. 3, 831–838. MR2142238

[Ste82] Glenn Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser Boston, Inc., Boston, MA, 1982. MR670070

[Sut] A. Sutherland, `http://math.mit.edu/~drew/X1_altcurves.html`

[Yan09] Yifan Yang, *Modular units and cuspidal divisor class groups of* $X_1(N)$, J. Algebra **322** (2009), no. 2, 514–553, DOI 10.1016/j.jalgebra.2009.04.012. MR2529102

Mathematisch Instituut Universiteit Leiden Niels Bohrweg 1 2333 CA Leiden Nederland

Current address: Mathematisches Institut Universität Bayreuth 95440 Bayreuth Deutschland

Email address: `maarten@mderickx.nl`

URL: `http://www.mderickx.nl`

Mathematics Department Harvard University 1 Oxford Street Cambridge, Massachusetts 02138

Email address: `mazur@math.harvard.edu`

URL: `http://www.math.harvard.edu/~mazur/`

Department of Mathematics University of Southern California 3620 South Vermont Ave. Los Angeles, California 90089-2532

Email address: `kamienny@usc.edu`

Licensed to AMS.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/publications/ebooks/terms