Some comments on elliptic curves over general number fields and Brill-Noether modular varieties

B. Mazur

July 20, 2014

Very rough notes for a lecture to be given October 5, 2013 at the Quebec/Maine Number Theory Conference. I'll discuss diophantine questions that take on a somewhat different flavor when one deals with varying number fields rather than restricts to $\mathbf{Q}$ *as a base field: an on-going joint project with Maarten Derickx and Sheldon Kamienny regarding Mordell-Weil torsion, and some recent work with Zev Klagsbrun and Karl Rubin (essentially) regarding Mordell-Weil rank.*

Contents

Consider elliptic curves E defined over number fields K, and denote by $E(K)$ the group of rational points in E with coefficients in K–i.e., the *Mordell-Weil group* of E over K. Since $E(K)$ is a finitely generated abelian group, we can write

$$E(K) \simeq T(E,K) \bigoplus \mathbf{Z}^{r(E,K)}$$

where $T(E,K)$, is the (finite abelian) torsion group of $E(K)$ and $r(E,K) \geq 0$ is the rank, these giving us two functions.

- $(E,K) \mapsto$ the isomorphy class of $T(E,K)$,

  and

- $(E,K) \mapsto r(E,K) \geq 0,$

whose statistics pose very interesting problems.

The question of the behavior and distribution of *Torsion* over varying E and K and of *Rank* over the same sample set give, in fact, two mathematical projects that are—as perhaps is no surprise—quite different.

1 Torsion

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. Thirty-five years ago I proved a theorem classifying prime $\mathbf{Q}$-rational torsion in the Mordell-Weil groups of elliptic curves (over $\mathbf{Q}$) and soon thereafter (with contributions from ***) one had the following classification:

Theorem 1. *$T(E,\mathbf{Q})$ is either cyclic of order ≤ 10, or order 12, or else is a direct product of a cyclic group of order 2 with a cyclic group of order $2, 4$ or 6.*

This, of course, is only over the field of rational numbers, $\mathbf{Q}$, but the natural profile of the question requires understanding torsion phenomena for *all* elliptic curves over *any* fixed number field K. Here we have some exciting results due to a number of people, Merel, Oesterlé, Parent, Kamienny,

and very recent progress due to Maarten Derickx, Sheldon Kamienny, William Stein, Michael Stoll, and van der Hoej. And yet there remains quite a project (computational exploration, and–of course—theoretical as well) to be done.

Fix a positive integer d and let $P(d)$ be the *largest* prime number p such that there exists an elliptic curve without CM (i.e., without 'extra' endomorphisms) defined over some number field of degree $\leq d$ over $\mathbf{Q}$ and for which there is a point of order p on that elliptic curve, rational over that field. Only for small d is $P(d)$ actually known.

- **Torsion over the field of rational numbers:** My theorem says that $P(1) = 7$ and was a solution of a conjecture of Andrew Ogg. Ogg conjectured, in effect, that there exist elliptic curves with torsion subgroup of a given type *if and only if* the corresponding modular curve that classifies such torsion is of genus zero. Another way of phrasing Ogg's conjecture is to say that any example of an elliptic curve over $\mathbf{Q}$ with rational torsion subgroup of a given isomorphy type is a member of a rationally parametrized such family giving infinitely many such examples.

- **Torsion over quadratic fields:** Since $X_1(11)$ is an elliptic curve, and therefore 'hyperelliptic over $\mathbf{Q}$' in the sense that it admits a degree two map to $\mathbf{P}^1$ (over $\mathbf{Q}$) it follows that there is a rationally parametrized family of elliptic curves possessing 11-torsion over quadratic number fields, so $P(2)$ is certainly ≥ 11. For fairly elementary reasons, again we have that any example of an elliptic curve over $\mathbf{Q}$ with rational 11-torsion over a quadratic field is a member of a rationally parametrized such family giving infinitely many such examples.

  Sheldon Kamienny proved that $P(2)$ is actually 13. So Derickx, Kamienny and I recently revisited Kamienny's theorem and we proved that—just as every example of rational torsion over $\mathbf{Q}$ is a member of a rationally parametrized family of infinitely many examples—the same is true for $d = 2$; i.e., every example of an elliptic curve with a rational torsion point of order any N over a quadratic number field is a member of a rationally parametrized family of infinitely many examples.

  To focus on this for more general situations let us make some (provisional) terminology:

  Definition 1. *If X is a curve over a field k, the* **k-gonality of** *X, denoted $d_k(X)$, is the minimal degree of a k-rational function on X. That is, $d_k(X)$ is the minimal degree of a function*

  $$X \to \mathbf{P}^1$$

  defined over k.

  In particular, there *is* a rationally parametrized one parameter family of points of X defined over fields of degree $d = d_k(X)$.

  Definition 2. *Letting $\bar{k}$ be the algebraic closure of k, a* **base rational function** *on a curve X defined over k is a rational function on X of degree $d = d_{\bar{k}}(X)$, noting that in such a case, $d_k(X) = d_{\bar{k}}(X)$.*

  For modular curves, the classical *Hauptmoduls* are instances of such, when the relevant modular curve is of genus 0.

For the **Q**-gonalities of the modular curves $X_1(N)$ with $N \leq 40$ see *Gonalities of Modular Curves*, a preprint of Maarten Derickx and Mark van Hoeij which are notes to a lecture they gave at the Intercity Number Theory Seminar 01-03-2013 (`http://mderickx.nl/slides/gonaliteiten.pdf`). In particular

$N = p$	13	17	19	23	29	31	37
$\mathrm{Q-gonality}$	2	4	5	7	11	12	18

Definition 3. *A rational (noncuspidal, non-CM) point of $X_1(N)$ over a number field of degree d is* **sporadic** *if $d \leq d_{\bar{k}}(X)$ and there is no* **Q***-rational map of $X_1(N)$ to $\mathbf{P}^1$ of degree d sending that point to a* **Q***-rational point in $\mathbf{P}^1$.*

Note that the sporadic points of $X_1(N)$ are preserved by the action of **Q**-automorphisms of $X_1(N)$ and therefore is closed under the action of Δ, the group of "diamond operators." See Mark van der Hoej's preprint *Low Degree Places on the Modular Curve $X_1(N)$* (`http://www.math.fsu.edu/~hoeij/files/X1N/LowDegreePlaces`) for a list of examples of rational torsion of elliptic curves of moderately low degree (completely explicitly given) that do not lie in families of such examples of the same low degree. For example, $N = p = 29$ is the first prime that appears in van der Hoej's list, where he found 3 diamond-orbits of sporadic (noncuspidal, non-CM) points, one for degree $d = 9$ and two for $d = 10$ (the gonality of $X_1(29)$ being 11).

So, for a (noncuspidal, non-CM) point to be *nonsporadic* it must be a member of a rationally parametrized family[1] of (small) degree d. My theorem then says that there is no sporadic point on any of the modular curves $X_1(N)$ of degree 1, and the joint work with Derickx and Kamienny says the same for degree 2.

A theorem of Abramovich gives that for $X = X_1(p)$ the **C**-gonality of X is $\asymp p^2$ and this suggests (to me) that for p large we may well expect quite an increasing quantity of sporadic points.

Let's go further with a description of recent work. Parent, building on work of Kamienny, showed $P(3) = 13$, and recently Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll showed that $P(4) = 17$.

- **Torsion over quartic fields:** Here, for the 'new prime,' $p = 17$, there are no sporadic elliptic curve examples (of 17-torsion over fields over degree ≤ 4). And as Derickx, Kamienny and I have recently shown:

  Theorem 2. *The only examples of* 17*-torsion on elliptic curves over quartic fields come from three distinct rationally parametrized (infinite) families of them.*

  We'll return to this result offering some precision to its statement. But

  The question of classifying base rational functions over a number field k is a diophantine question. Specifically, recall that the **Brill-Noether variety**, $W^r_\delta X$, of a smooth projective curve X (over k) is the subvariety

$$W^r_\delta(X) \subset \mathrm{Pic}^d(X)$$

[1] I call the terminology 'provisional' because of the embarrassment that an infinite family of such examples that happen to be parametrized by infinitely many points on an elliptic curve, would—by our definition—still be called "sporadic." Regarding this, one might mention the theorem of Frey that guarantees that such infinitely many sporadic points will only occur in degrees greater than or equal to one half the **Q**-gonality of $X_1(N)$.

that classifies what the algebraic geometers call g^r_δ's for the curve X. That is, effective divisors of degree δ on X living in linear systems of dimension $\geq r+1$. So, $W^1_\delta X$ classifies effective divisors of degree δ on X that actually do live in a positive-dimensional linear system.

Definition 4. *By the* **Basic Brill-Noether variety**, *WX, of a smooth projective curve X (over a number field k) let us mean the classical Brill-Noether variety W^1_δ (defined over k) where we take δ to be the smallest degree such that the variety $W^1_\delta(X)$ is nonempty.*

Lemma 1. *That smallest δ is equal to $\delta = d_{\bar{k}}(X)$.*

Proof. Clearly $\delta \leq d_{\bar{k}}(X)$, so we must show the reverse inequality. Since $d_{\bar{k}}(X) = d_{\mathbf{C}}(X)$ and the "δ" is insensitive to whether we are working over $\bar{k}$ or $\mathbf{C}$, without loss of generality we may assume that our base field is $\mathbf{C}$ and we'll just talk about points on the associated Riemann surfaces. Suppose there exists a g^1_δ, giving us a linear system of effective divisors,

$$D_t = \sum_{i=1}^{\delta} x_{i,t},$$

for points $x_{i,t} \in X(\mathbf{C})$, with t a parameter for $\mathbf{P}^1$. Noting that $D_t \neq D_{t'}$ and $D_t \equiv D_{t'}$ for any two distinct points $t, t' \in \mathbf{P}^1$, and noting that δ is the minimal degree for which there is a positive dimensional linear system with effective divisors of that degree, we see that for $t \neq t'$, the sets (allowing possible multiplicities)

$$\{x_{1,t}, x_{2,t}, \ldots, x_{\delta,t}\}$$

and

$$\{x_{1,t'}, x_{2,t'}, \ldots, x_{\delta,t'}\}$$

must be disjoint. For, if not— e.g., if $x_{1,t'} = x_{1,t}$, we would get a linear equivalence relation between the effective divisors $D_t - x_{1,t}$ and $D_{t'} - x_{1,t'}$ (which are **(a)** distinct and **(b)** of degree less that δ. It follows that any point x in X is in the support of a unique D_t and this (well-)defines a mapping $x \mapsto t$, i.e., a base rational function on X.

This establishes an identification:

$$WX(k) \quad \longleftrightarrow \quad \textbf{Equivalence-classes of base rational functions on } X \textbf{ over } k\textbf{.}$$

"Equivalence classes" means up to composition with linear fractional transformations of the range (defined over k). The identification is compatible with the natural action of the automorphism group $\mathrm{Aut}_k(X)$ (acting by composition on base rational functions, and by functoriality as a group of k-rational automorphisms of WX).

Taking X to be $X_1(N)$ forthcoming joint work with Maarten Derickx and Sheldon Kamienny studies what we call *basic Brill-Noether modular variety* $WX_1(N)$, which inherits a lot of the structure (e.g., the dihedral group of automorphism built out of the $\mathbf{Q}$-rational "diamond operators," and also the "w operators") and we'll get to an example of this shortly.

- **Torsion over fields of higher degree:** One knows that $P(5) = 19$ and, all primes $p \leq 19$ occur as rational p-torsion for some elliptic curve defined over some field of degree ≤ 5.

  But what about results for general values of d?

Here we have the deep theorem of Merel that for any d, $P(d) < \infty$. For a more specific upper bound, Merel's work with improvements from Oesterlé and Parent shows—for general d—that

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

Or, to round it out,

$$P(d) << 3^d.$$

An exponential bound, in other words.

To gauge how close this upper bound comes to the actual phenomena, let's contemplate lower bounds. The trivial lower bound is

$$(*) \quad d^{1/2} << P(d),$$

and here's a proof of this. Take any elliptic curve E over $\mathbf{Q}$ and note that over $\bar{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$, the kernel of multiplication by p in E is a (p,p)-type group, i.e., a two dimensional vector space over the prime field $\mathbf{F}_p$ and the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on this vector space through a subgroup of the general linear group $\Gamma \subset \mathrm{GL}_2(\mathbf{F}_p)$. If you pass to an extension field $K/\mathbf{Q}$ such that the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$ acts through a subgroup Δ of triangular matrices of the form

$$\begin{bmatrix} 1 & * \\ * & * \end{bmatrix}$$

then E will have a torsion point of order p rational over this K. Since $[\mathrm{GL}_2(\mathbf{F}_p) : \Delta] = p^2 - 1) = O(p^2)$, the degree of such a K is $\leq p^2$, which gives **(*)**.

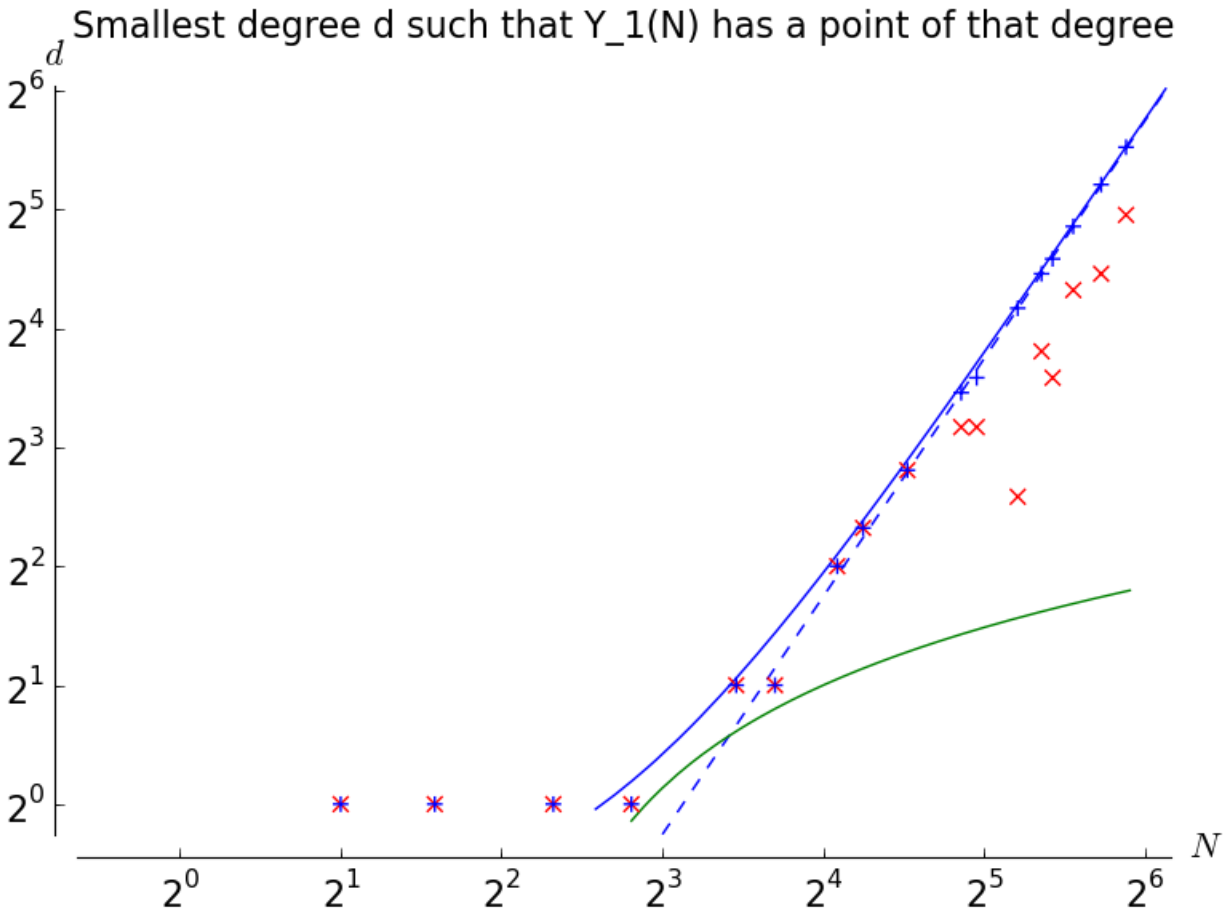
Note: A more geometric way of saying exactly the same thing is to make use of the natural mapping—defined over $\mathbf{Q}$—of the modular curve $X_1(p)$ to the j-line, which is is of degree $O(p^2)$.

So we have

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

Since no other wholesale construction of larger p-torsion in fields of degree d comes to mind, the minimalist instinct would then nudge one to consider the possibility that there would be a polynomial, rather than exponential upper bound for $P(d)$, and perhaps even an upper bound of the form $P(d) << d^{1/2+\epsilon}$.

Here below is a graph computed by the first author of the present article jointly with Mark van Hoej. 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.



In the literature, some conjectures give upper bounds for primes of torsion in elliptic curves of degree d, but since these published conjectures also consider prime torsion in CM elliptic curves, which our "$P(d)$" doesn't register, those conjectures necessarily must allow for an essentially linear lower bound[2].

Explicitly,

Conjecture 1. *(Clark, Cook, J. Stankewicz)*

$$P(d) \ << \ d \log\log(d),$$

Conjecture 2. *(Lozano-Robledo)*

$$P(d) \ << \ d.$$

It is tempting, then, to focus on the exponent of d related to the rate of increase of $P(d)$, i.e., to define:

$$e(d) := \frac{\log P(d)}{\log d}$$

[2] One might imagine distinctive bimodal behavior, for prime torsion in elliptic curves without CM over fields of degree d versus prime torsion in elliptic curves with CM.

and to ask:

Question 1. *Can one find infinitely many values of d with $e(d)$ strictly greater than $\frac{1}{2}$?*

2 Focusing on $p = 17$ and quartic fields

The modular curve $X := X_1(17)$ is of genus 5, that have the following basic features that help us get into their arithmetic efficiently.

- The $\mathbf{Q}$-gonalities, and $\mathbf{C}$-gonalities are all equal ($\delta(X) := \delta_{\mathbf{Q}}(X) = \delta_{\mathbf{C}}(X) = 4$),
- X has no noncuspidal points of degree ≤ 3 and
- the basic Brill-Noether variety X is a curve.

A further valuable resource in studying this case is that people have computed elegant equations for $X_1(17)$. (See Sutherland's list for a number of modular curves in `http://math.mit.edu/~drew/X1_altcurves.html`. The equation Sutherland gives for $X_1(17)$ was initially found (as we understand it) by Cadey and Elkies, and is particularly crisp: the formula

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

is a ("biprojective") birational morphism of $X_1(17)$ onto a curve in $\mathbf{P}^1 \times \mathbf{P}^1$ of bidegree $(4, 4)$. This morphism is an embedding of 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 $x := E_5E_6/E_1{E_3}^3$ and the projection to the second factor is given by the modular unit $y := E_6E_7/E_2E_8$.

The parameters $x : X_1(17) \to \mathbf{P}^1$ and $y : X_1(17) \to \mathbf{P}^1$ in the equation **(*)** provide two rational families of elliptic curves defined over fields of degree 4 possessing points of order 17 (rational over those degree four fields). Consider the function of degree four, $z : X_1(17) \to \mathbf{P}^1$, given by the formula:

$$(*) \quad z := \text{ to be included.}$$

Maarten Derickx, Sheldon Kamienny and I prove (based, of course, on the results already mentioned) is the following:

[3] Here we are using the notation of Siegel units E_n by Yang, following Kubert-Lang. The identification of x and y as Siegel units are taken from a table computed by Burton Newman.

Theorem 3. *The rational parameters x, y, z give, up to* **Q***-similarity*[4] *all* **Q***-rational parametrizations of $X_1(17)$ of degree equal to its gonality (i.e., degree = 4). The Galois group of the finite extension*

$$x : X_1(17) \to \mathbf{P}^1$$

is the full symmetric group[5] *S_4 while the finite mappings*

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

factor through the bi-elliptic representation

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

Now the fun here is that there are, in fact, two distinct ways of getting at the diophantine problem involved. And they dovetail in a nice way. We can approach the problem either by considering:

- **Q**-rational points on the Basic Brill-Noether modular curve WX,

or

- rational cuspidal divisors and "fine" Siegel units.

2.1 Via the Basic Brill-Noether modular curve

The Basic Brill-Noether modular curve $W := WX_1(17)$ is a double cover of a plane quintic (reducible) curve

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

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 $W \to V$—well known to algebraic geometers—as obtained from the canonical representation of $X = X_1(17)$ which provides the neat way of computing the equations $(*)$, and which we'll now describe.

The group, Δ, of 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 **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

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

[5] 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.

$(x-1)(x^4+1)$, this means that there is a unique basis $\omega_0, \ldots, \omega_4 \in S_2$ such that with respect to this basis we have:

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

This basis is given by

$$\omega_0 := q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 + O(q^9) \quad (1)$$
$$\omega_1 := q - q^2 - q^3 + q^6 - q^7 + q^8 + O(q^9) \quad (2)$$
$$\omega_2 := q^2 - q^3 - 2q^4 + q^5 + q^6 + q^7 + O(q^9) \quad (3)$$
$$\omega_3 := -q^2 + q^3 + q^4 + q^5 - q^6 - q^7 - q^8 + O(q^9) \quad (4)$$
$$\omega_4 := q^3 - 2q^4 + q^6 - q^7 + 3q^8 + O(q^9) \quad (5)$$

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

$$e_0 := \omega_0^2 - \omega_1^2 - \omega_2^2 - \omega_3^2 - \omega_4^2 \quad (6)$$
$$e_1 := 2\omega_1\omega_2 + 2\omega_1\omega_3 - 2\omega_3\omega_4 \quad (7)$$
$$e_2 := 2\omega_2\omega_3 + 2\omega_1\omega_4 + 2\omega_2\omega_4 \quad (8)$$

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, has four rational points all of which yield parametrizations in the $\mathbf{Q}$-similarity class of the parametrization y above, and all this is directly related to the bi-elliptic representation of $X_1(17)$. (We'll discuss this in a moment.) 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

$$2Y^2Z + 2XY^2 + XZ^2 - X^3$$

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 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:

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

  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 contribute to the single $\mathbf{Q}$-similarity class represented by the function "y" 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 **(*)** by the following route. 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.

2.2 Via Fine Siegel units

Here an utterly independent way of making this computation by noting that the only sparce points on $X_1(17)$ are the eight rational cusps, and therefore any $\mathbf{Q}$-rational function f of degree 4 on $X_1(17)$ has the curious requirement 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 f with an appropriate $\mathbf{Q}$-automorphism of $\mathbf{P}^1$ one can get a $\mathbf{Q}$-rational function f' of degree 4 on $X_1(17)$ whose divisor of zeroes and poles consist entirely of rational cusps. Call such a function 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. This, of course, is a finite computation, and as an example, the function "x" of the theorem has precisely three rational cuspidal fibers. The multiplicity of each of the eight rational cusps, in the three rational cuspidal fibers is describable as the following 8×3 matrix M. Here the cusps are labeled in the traditional way, and ordered as :

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

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

Depending on how you decide to parametrize this; i.e., which one:one correspondence you choose to send the three rational cuspidal fibers to the subset $\{0, 1, \infty\} \subset \mathbf{C}$ you get $\mathbf{Q}$-linear parameterizations of $X_1(17)$ given by different fine Siegel units. For example E_1E_3/E_5E_6 has the first row of M 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 as zero-divisor and the second row as polar-divisor.

3 "Siegel points"

Definition 5. *By a* **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 (*$\mathbf{Q}$*-rational) Siegel*

unit, and call it a **Fine Siegel point** *if it is represented by a fine Siegel unit.*

In the case, then, of $N = 17$, 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 der Hoej (see loc. cit.) 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 $\mathbf{C}$-gonality of $X_1(N)$, the corresponding Basic Brill-Noether variety $WX_1(N)$ would contain at least one Siegel point.

4 Two side-comments about diophantine questions over varying number fields

Noting that we have been discussing new feature of diophantine problems that arise when we consider varying fields of definition, let me end with comments about two other such questions.

4.1 Disparity of rank over general number fields

The problem of parity of rank has a (surprising) new feature when considered for more general number fields rather than just $\mathbf{Q}$. This is described in recent work of Zev Klagsbrun, Karl Rubin and myself. We deal with the mod 2-Selmer rank parity for a quadratic twist family over a number field K. This, then, is conjecturally the Mordell-Weil rank parity. If one formulates parity density questions over *all* elliptic curves over any fixed number field, one expects 50/50 as the answer. If you pose the question just for any quadratic twist family of a given elliptic curve over $\mathbf{Q}$, one expects the same result: 50/50. We show that in the case where the number field K has at least one real embedding, the distribution of even/odd parities is 50/50.

BUT even if you fix a specific elliptic curve E and allow different choices of field K over which you gather parity statistics, the proportions of even/odd can change dramatically. For example, take the elliptic curve (labelled 50B1 by Cremona)

$$E: \quad y^2 + xy + y \;=\; x^3 + x^2 - 3x - 1.$$

By judicious choices of fields K one can obtain quadratic twist families whose mod 2-Selmer rank parity ratios take on a dense set of numbers in the range $(0, 1)$.

4.2 The question of undecidability

These issues are usually phrased over a given number field (usually $\mathbf{Q}$ is interesting enough) and for a large collection of systems of equations, or varieties. If you flip the quantification, though, by

simply *fixing* X to be any (projective smooth) finite union of genus ≥ 2 curves over a number field K the question of constructing all L-rational points over *all* number field extensions of K is—to my knowledge—currently not achieved for any single example. It is easy to reconstrue this question as a question for such curves X defined only over $\bar{\mathbf{Q}}$. It seems to me that even *relative decidability* is *almost* a total mystery when one asks the question for all number fields, and beyond the trivial fact that if $X' \to X$ is an explicit mapping of finite degree between two such curves, a solution the diophantine decidability question for X implies the same for X'.

For fun, but without even a firm conjecture in mind, one can formulate the question more broadly this way. For any geometrically irreducible curve X (smooth, and projective) over a number field $K \subset \bar{\mathbf{Q}}$ say that $d \geq 1$ is a *low degree* for X if $\mathrm{Symm}^d(X)$ contains no subvarieties over $\bar{\mathbf{Q}}$ isomorphic to an abelian variety of positive dimension, or to a rational curve.

If X has "low degree" $d \geq 1$, then it is of genus ≥ 2 and therefore has a canonical embedding, and a corresponding canonical height function on its algebraic points. Moreover, by a theorem of Faltings, $\mathrm{Symm}^d(X)$ has only finitely many rational points over any number field extension L of K, and any such point can be viewed as a (collection of) algebraic points on X of degrees $\leq d$ over L.

Now consider schemes

$$Z = \cup_{j=1}^{\nu} \mathrm{Symm}^{d_j}(X_j)$$

in $\mathcal{C}$, where the X_j's are projective smooth curves over $\bar{\mathbf{Q}}$ and the d_j's are low degrees for their X_j'. Fix any model of Z over some number field K. Then for a number field extension L/K we may regard the (finitely many) L-rational points of Z as giving algebraic points (of various degrees) on the various curves X_j. Define, then, a real-valued function of number field extensions L/K,

$$h_{Z,K} : L/K \longrightarrow \mathbf{R},$$

by the rule: $h_{Z,K}(L/K)$ is the maximum canonical height of any of these algebraic points comprising the L-rational points of Z. Given another model of Z over another number field K', the two functions $h_{Z,K}, h_{Z,K'}$ are 'eventually equal' in the sense that there exists a sufficiently large number field L_o containing both K and K' so that $h_{Z,K}$ and $h_{Z,K'}$ have the same values for all extensions L/L_o.

We may think of a decision procedure for the rational points of such a Z to be a (proved) upper bound

$$h_{Z,K} \leq H_{Z,K}.$$

where $H_{Z,K}$ is a computable positive integer valued function of number field extensions L/K, with "computable" taken to be any specific one of its standard possible meanings.

More flexible would be to imagine relative decision procedures, where one is given two objects Z and Y of our category and wishes to obtain a decision procedure for Z, given Y as an "oracle." Say then that

$$Y \geq_{\mathrm{Diophantine}} Z$$

if we have a (proved) upper bound

$$h_{Z,K} \leq H_{Z,K} \circ h_{Y,K}.$$

where $H_{Z,K}$ is a computable positive integer valued function of number field extensions. The partial ordering "$\geq_{\text{Diophantine}}$" is independent of the model of Z over$K$, or the particular number field K. Moreover, if we have an explicit finite morphism $Z \to Y$ in our category, then $Y \geq_{\text{Diophantine}} Z$. Are there other times when $Y \geq_{\text{Diophantine}} Z$?