Heegner point computations over function fields

Mihran Papikian
Department of Mathematics
University of Michigan, Ann Arbor, MI 48109

Abstract

These are the notes of an expanded version of the project done under the direction of Douglas Ulmer at Arizona Winter School 2000 - *The Arithmetic of Function Fields*. We carefully explain how to compute explicitly the Heegner points for an elliptic curve defined over $\mathbf{F}_2(T)$.

1 Introduction

Let $F = \mathbf{F}_q(T)$ be the rational function field over $\mathbf{F}_q$. For every $N \in \mathbf{F}_q[T]$ there exists a coarse moduli scheme $Y_0(N)$ over $\mathbf{F}_q[T]$ parametrizing isomorphism classes of pairs (ϕ, ϕ') of Drinfeld modules of rank 2 together with a cyclic isogeny $u \ : \ \phi \to \phi'$ of degree N. This means that $\ker u \cong \mathbf{F}_q[T]/(N)$. $Y_0(N)$ can be compactified to a scheme $X_0(N)$ by adjoining a finite number of sections. The points of these sections can be interpreted as generalized Drinfeld modules. $X_0(N)_{/F}$ is a smooth irreducible projective curve over F.

Now let K be an imaginary quadratic extension of F (i.e. a fixed place ∞ does not split), and let N be such that each of its prime divisors is split in K. Suppose that ϕ, ϕ' are two Drinfeld modules of rank 2 for the ring $\mathbf{F}_q[T]$ with complex multiplication by the maximal order $\mathcal{O}_K$ of K, i.e. $End\ \phi = End\ \phi' = \mathcal{O}_K$, and that $u \ : \ \phi \to \phi'$ is a cyclic isogeny of degree N. The triple (ϕ, ϕ', u) defines a point x on $X_0(N)(F^{sep})$, and in fact it is rational over the Hilbert class field H of K relative to ∞ (that is, the maximal unramified abelian extension which is split completely at ∞). Such points are called *Heegner points*. The usefulness of Heegner points for the arithmetic of elliptic curves comes from the following fundamental result

Theorem 1.1 (Deligne - Drinfeld - Zarhin) *For each elliptic curve E/F with split multiplicative reduction at ∞ and conductor $N_E = N \cdot \infty$ there is a non-trivial morphism $\wp \ : \ X_0(N) \to E$.*

Denote by P the image of a Heegner point under the modular parametrization, in particular $P \in E(H)$. Put $P_K = Tr_{H/K} P \in E(K)$. Then

Theorem 1.2 (Gross-Zagier formula for function fields)

$$< P_K, P_K >_K = c \cdot \frac{\partial}{\partial s} L(E/K, s)|_{s=1}$$

where $< P_K, P_K >_K$ *is the canonical (or Neron-Tate) height of* P_K *computed over* K *and* c *is a non-zero constant (a priori depending on the choice of the modular parametrization)*

This theorem has been proved by Rück and Tipp for $F = \mathbf{F}_q(T)$ and char $F \neq 2$ [10], and by D. Ulmer for general function fields of smooth projective curves over a finite field (the proof was announced during Arizona Winter School 2000, and will appear in a subsequent monograph).

The Gross-Zagier formula in function field setting is enough to prove Birch and Swinnerton-Dyer conjecture for elliptic curves over K of analytic rank ≤ 1. In particular, Kolyvagin type arguments are redundant for function fields once (1.2) is true. Indeed, $L'(E/K, 1) \neq 1 \Longleftrightarrow < P_K, P_K >_K \neq 0$ $\Longleftrightarrow P_K$ has infinite order in $E(K) \Longrightarrow$ rank $E(K) \geq 1$. But a priori, thanks to a result of Tate [14], rank $E(K) \leq \text{ord}_{s=1} L(E/K, s) \Longrightarrow$ rank $E(K) = \text{ord}_{s=1} L(E/K, s)$. The refined version of BSD, which specifies the leading Taylor coefficient of $L(E/K, s)$, follows from the results of Tate and Milne [14], [7], [8], see section 7 for more details. To prove BSD for E over F one has to use non-vanishing theorems of twists of L-functions.

We should also mention that in fact Kolyvagin's arguments were transferred to function fields by M. Brown in [1]. For $F = \mathbf{F}_q(T)$ and char $F \neq 2$ he proves, using Euler systems of Heegner points, that if P_K is non-torsion then rank $E(K) = 1$. The paper very closely follows the argument given by B. Gross in [2].

This paper contains a write up of an expanded version of the project I did under the direction of D. Ulmer at AWS 2000. The goal of the project was to directly verify BSD, and the Gross-Zagier formula for function fields for one concrete example, including an explicit calculation of the constant c in (1.2). It is done in two ways. The first proceeds by computing the equation of the Drinfeld modular curve $X_0(N)$ parametrizing our elliptic curve. The second uses the explicit formulae worked out by Gekeler and Reversat [5] for $X_0(N) \longrightarrow E$. The second approach seems more appropriate if one wishes to calculate the Heegner points in more general situation, as the equation for $X_0(N)$ gets very complicated. Although we should mention that actual approximation of the values of theta series used in [5] is also very time consuming (for our simple example it took approximately one hour on a UNIX machine), and one has to be able to produce concrete generators for Schottky groups, which by itself seems to be a rather hard problem, see [9].

The example we consider is the following. Let $F = \mathbf{F}_2(T)$, and consider the elliptic curve E

over F with affine equation

$$Y^2 + TXY = X^3 + T^2X \tag{1}$$

and its quadratic twist E' with affine equation

$$Y^2 + TXY = X^3 + T^3X^2 + T^2X \tag{2}$$

The quadratic extension is $K = F(U)$ where $U^2 + U = T$. The isomorphism between E and E' is given by substituting $Y := Y' + (U^3 + U)X$ into the equation for E'.

Why this particular choice of E? It is reasonable to choose the field of constants to be small like $\mathbf{F}_2$, to be able to compute, for example, the L-function by hand. Also in case of $\mathbf{F}_2(T)$, up to coordinate change in T, there are precisely two different N such that $X_0(N)$ has genus one. One of them is $N = T^3$. We will see that E has conductor $T^3\infty$ and it turns out that $X_0(N) = E$ which simplifies many of the technical details.

Also observe that since in our example char $F = 2$ neither [10] nor [1] applies. Nevertheless, not only we verify that the Heegner point has infinite order and rank $E(K) = \mathrm{ord}_{s=1}L(E/K, s) = 1$, but also our explicit calculation of the constant c in (1.2) very nicely matches the constant worked out by Rück and Tipp except one has to replace Kummer extensions by Artin-Schreier extensions.

2 Elementary Invariants

The main purpose of this section is to compute the conductor and the component groups of E and its twist E'. These computations will be essential for later sections. The reference for this section is Tate's article [13].

$$E: \qquad Y^2 + TXY = X^3 + T^2X$$

One easily computes $\Delta = T^8$, and $j = T^4$. It has an additive reduction at $T = 0$. Tate's algorithm [13] shows that the reduction type is I_1^* in Kodaira's notation, i.e. this fibre of a minimal proper regular model of E has 6 irreducible components, four of which occur with multiplicity one. Component group is $\mathbf{Z}/4$, and it is all rational over k_T. The degree of T in the conductor is 3.

To find out the reduction type at infinity substitute $1/T$ for T in 1, after normalization (to the Weierstass form) the equation becomes

$$Y^2 + XY = X^3 + T^2X, \tag{3}$$

with $\Delta = T^4$, and $j = 1/T^4$. It has a split multiplicative reduction at $T = 0$, and the reduction type is (again from Tate's algorithm) I_4. This special fibre has 4 irreducible components each with multiplicity 1. The component group is $\mathbf{Z}/4$. So ∞ in the conductor shows up with degree 1.

Finally, the conductor of E is

$$N_E = T^3 \cdot \infty.$$

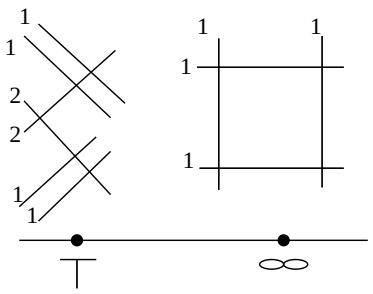


Figure 1: Special fibres on E

Similarly for

$$E' : \qquad Y^2 + TXY = X^3 + T^3X^2 + T^2X$$

$\Delta = T^8$, and $j = T^4$. It has a cuspidal reduction at $T = 0$. Tate's algorithm shows that the reduction type is I_1^*. The component group is $\mathbf{Z}/4$, and it is constant. The degree of T in the conductor is 3.

To find the reduction type at infinity again substitute $1/T$ for T in (2), after normalization (to the Weierstass form) the equation becomes

$$Y^2 + TXY = X^3 + TX^2 + T^6X, \tag{4}$$

with $\Delta = T^{16}$, and $j = 1/T^4$. This equation is not in its minimal form (e.g. $val_T(\Delta) > 12$) but we don't care as Tate's algorithm will tell us if this affects the reduction type. It has a cusp at $T = 0$, and the reduction type is I_8^* (this takes for a while to compute as one has to blow up 13 times). The special fibre has 13 irreducible components only four with multiplicity 1. The component group is $\mathbf{Z}/2 \times \mathbf{Z}/2$, it is again rational, and ∞ in the conductor occurs with degree 4.

Finally, the conductor of E' is

$$N_{E'} = T^3 \cdot \infty^4.$$

3 $E(F)$ and $E'(F)$ as groups

In this section we describe $E(F)$ and $E'(F)$ as abelian groups. The hard part is to get a handle on the ranks of these groups. To do so we compute the L-functions of our curves and use the Tate's

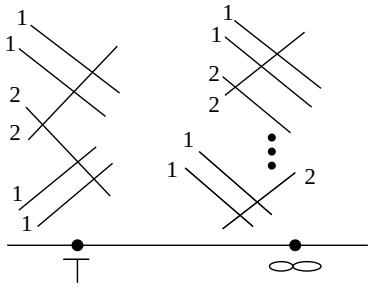


Figure 2: Special fibres on E'

result bounding the rank of a non-isotrivial elliptic curve over a function field F by the order of vanishing of the L-function at $s = 1$:

$$\text{rank } E(F) \leq \text{ord}_{s=1} L(E/F, s) \tag{5}$$

(Of course, Birch and Swinnerton-Dyer conjecture implies that equality always holds).

Computing the right hand-side of (5) is quite straightforward thanks to Grothendieck's cohomological interpretation of L-functions.

This approach is rather specific to function fields. Over number fields to get a bound on the rank of $E(F)$ one has to apply computationally more elaborate descent arguments, c.f. [11] Ch.X.

Let E be an elliptic curve over $\mathbf{F}_q(T)$ of conductor N_E. We first recall the definition of the L-function of E.

For a divisor $\mathfrak{p}$ denote by $|\mathfrak{p}|$ the norm with respect to ∞-adic valuation (i.e. $|\mathfrak{p}| = \mathfrak{q}^{\deg \mathfrak{p}}$). For a place $\mathfrak{p} \not| N_E$ of F define

$$a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#E_{\mathfrak{p}}$$

where $\#E_{\mathfrak{p}}$ is the number of points of the reduction of E at $\mathfrak{p}$ over $\mathbf{F}_{\mathfrak{p}}$

$$a_{\mathfrak{p}} = \alpha_{\mathfrak{p}} + \overline{\alpha_{\mathfrak{p}}}, \quad \alpha_{\mathfrak{p}} \in \mathbb{C}$$

such that $|\alpha_{\mathfrak{p}}| = |\mathfrak{p}|^{1/2}$, and for $\mathfrak{p}|N_E$ define

$$a_{\mathfrak{p}} = 0, 1, -1$$

according to if E has additive, split multiplicative or non-split multiplicative reduction. Then

$$L(E, s) = \prod_{\mathfrak{p}|N_E} \left(1 - \frac{a_{\mathfrak{p}}}{|\mathfrak{p}|^s}\right)^{-1} \prod_{\mathfrak{p}\not|N_E} \left(1 - \frac{\alpha_{\mathfrak{p}}}{|\mathfrak{p}|^s}\right)^{-1} \left(1 - \frac{\overline{\alpha_{\mathfrak{p}}}}{|\mathfrak{p}|^s}\right)^{-1}$$

$L(E,s)$ is also the $L-$function of the ℓ-adic representation ($\ell \neq$ char F) of $Gal(F^{sep}/F)$ acting on the dual of the Tate module of E

$$L(E,s) = \prod_{\mathfrak{p}} \det\left(1 - q^{-s}\ Frob_{\mathfrak{p}} \mid V_\ell(E)^{\vee I_{\overline{\mathfrak{p}}}}\right)^{-1}$$

where $I_{\overline{\mathfrak{p}}}$ is the inertia subgroup at $\mathfrak{p}$ and $V_\ell(E)^{\vee I_{\overline{\mathfrak{p}}}} = V_\ell(E)^\vee$ at the places of good reduction.

But even more important interpretation comes from Grothendieck's theory of L-functions.

$V_\ell(E)$ defines a constructible twisted-constant ℓ-adic sheaf on the places of $\mathbf{P}^1_{\mathbf{F}_q}$ where E has a good reduction, moreover

$$L(E,s) = \frac{P_1(q^{-s})}{P_0(q^{-s})P_2(q^{-s})}$$

$$P_j(X) = \det\left(1 - X\ Frob_q \mid H^j_{et}(\mathbf{P}^1_{\overline{\mathbf{F}}_q}, V_\ell(E)^\vee)\right).$$

$P_j(X) \in \mathbf{Q}[X]$ and $P_j(0) = 1$, $Frob_q$ corresponds to the global Frobenius. It is a standard fact that when E is non-isotrivial $P_0(X) = P_2(X) = 1$, moreover the degree of $P_1(X)$ is $\deg N_E - 4$. The functional equation is

$$L(E, 2-s) = \pm q^{(s-1)(\deg N_E - 4)} L(E,s)$$

Now returning to our example: $F = \mathbf{F}_2(T)$, E is the elliptic curve (1) and E' is its quadratic twist (2).

Since $N_E = T^3 \cdot \infty$ the degree of the conductor $\deg N_E$ (as a divisor) is 4. Thus

$$L(E/F, s) = 1$$

(as was explained above $L(E/F,s)$ is a polynomial in 2^{-s} of degree $4-4=0$ and constant term 1).

Similarly

$$L(E'/F, s) = 1 + c_1 2^{-s} + c_2 2^{-2s} + c_3 2^{-3s}.$$

The functional equation yields

$$2^{3s-3} L(E'/F, s) = -L(E'/F, 2-s)$$

(the sign is negative since the sign in the functional equation of $L(E/F,s)$ is trivially $+$ and E' is an imaginary quadratic twist of E).

By computing $\#\widetilde{E}'(k_{T+1}) = 2$, we get $c_1 = 1$, and using the functional equation we get $c_2 = -2$, $c_3 = -8$. So

$$L(E'/F, s) = 1 + 2^{-s} - 2 \cdot 2^{-2s} - 8 \cdot 2^{-3s}.$$

Now one easily computes that $L(E'/F, 1) = 0$, and

$$L'(E'/F, 1) = 7/2 \log 2 \neq 0. \tag{6}$$

Applying (5) to our curves we have

$$\text{rank } E(F) = 0 \qquad \text{and} \qquad \text{rank } E'(F) \leq 1.$$

This is enough to completely describe $E(F)$ and $E'(F)$ as we proceed to do. First of all, since rank $E(F) = 0$, E over F is a torsion group. Next we want to find prime-to-2 torsion. For that it is enough to reduce modulo few places as prime-to-2 torsion injects into $\widetilde{E}$ when $\widetilde{E}$ is nonsingular. But at $T + 1$, $\widetilde{E}: \ Y^2 + XY = X^3 + X$ has 4 points, so E has no prime-to-2 torsion.

The following points $(0, 0)$, $(T, 0)$, (T, T^2) are on E. Moreover $(0, 0)$ is of order 2, and $(T, 0)$, (T, T^2) are of order 4. To check that E has no 8-torsion, check that

$$X([2]P) = \frac{x^4 - T^4}{T^2 x^2} = T$$

has no solutions in F. This involves an elementary descent argument on the degrees of polynomials in the numerator and denominator of x. So

$$E(F) \cong \mathbf{Z}/4\mathbf{Z} \qquad \text{generated by} \quad (T, 0).$$

Similar analysis shows that torsion on E' is $\mathbf{Z}/2\mathbf{Z}$ generated by $(0, 0)$. Now some search reveals that $P = (T^3 + T, T^3 + T^2)$ is on E', and is integral of lowest degree.

$$E'(F) \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}.$$

Later, from height computations, we will show that P generates the infinite part of E'.

4 Computing the height pairing

The purpose of this section is to compute the *canonical* (or Neron-Tate) height of $P = (T^3 + T, T^3 + T^2)$ on E'. To do this we use the geometric construction of the canonical height due to Manin, c.f. [12] III.9.3.

Let $\mathcal{E}' \longrightarrow \mathbf{P}^1$ be a regular minimal elliptic surface, such that E'/F is the associated elliptic curve over $F = k(\mathbf{P}^1)$ (i.e. is the generic fibre of $\mathcal{E}'$). $\mathcal{E}'$ is a projective surface over $\mathbf{F}_2$, and each point P of $E(F)$ extends to a horizontal divisor (or a section) (P) on $\mathcal{E}'$, and the height of P is related to the self-intersection of a certain divisor on $\mathcal{E}'$. For the definition of intersection pairing as well as the terminology we use in this section we refer to [12], Ch. III, and [6], Ch. V.

For each point $P \in E'$, let $\Phi_P \in Div(\mathcal{E}') \otimes \mathbf{Q}$ be a fibral divisor so that the divisor

$$D_P = (P) - (O) + \Phi_P$$

satisfies $D_P \cdot \mathcal{F} = 0$ for all fibral divisors $\mathcal{F} \in Div(\mathcal{E}')$. Then Manin's formula for the canonical height pairing [12], III.9.3 is the following

$$< P, P >= -D_P \cdot D_P \log q \tag{7}$$

So to compute the height we have to compute Φ_P. One has to worry only about special fibres as $((P) - (O)) \cdot \mathcal{F} = 0$ for any good fibre $\mathcal{F}$.

Now we apply this to compute $< P, P >$, where $P = (T^3+T, T^3+T^2)$ is on $E' : \quad Y^2+TXY = X^3 + T^3X^2 + T^2X$. First note that P as a horizontal section passes through the singularity both at $T = 0$ and $T = \infty$ (at ∞ P looks like $(T^3 + T, T^4 + T^3)$, the equation for E' as in (4)). Hence when we desingularize E' by blowing up, P and O sections will pass through different irreducible components of multiplicity 1 in the special fibres of $\mathcal{E}'$.

Let $\mathcal{F}_0$ be the I_1^* fibre. The intersection of $\mathcal{F}_0$ with any other fibral divisor on $\mathcal{E}'$ is 0. In particular (for notations see Fig.3),

$$0 = A_i^0 \cdot \mathcal{F}_0 = A_i^0(A_1^0 + A_2^0 + A_3^0 + A_4^0 + 2B_1^0 + 2B_2^0) = (A_i^0)^2 + 2$$

Hence

$$(A_i^0)^2 = -2$$

Similarly,

$$0 = B_i^0 \cdot \mathcal{F}_0 = 1 + 1 + 2 + 2(B_i^0)^2 \Longrightarrow (B_i^0)^2 = -2$$

The same argument for ∞ gives

$$(A_i^\infty)^2 = -2, \qquad (B_i^\infty)^2 = -2$$

For our computations we also need the self-intersection of $(O) \cdot (O)$. Using the adjunction formula [6], V.1.5,

$$(O)^2 = -\deg(\Omega^1_{\mathcal{E}'/\mathbf{P^1}})|_O,$$

where $\Omega^1_{\mathcal{E}'/\mathbf{P^1}}|_O$ is the sheaf of relative 1-forms restricted to the O-section.

To be able to restrict to the O-section make a change of variables $X = \frac{u}{v}$, $Y = \frac{1}{v}$. The equation becomes

$$v + Tuv = u^3 + T^3u^2v + T^2uv^2$$

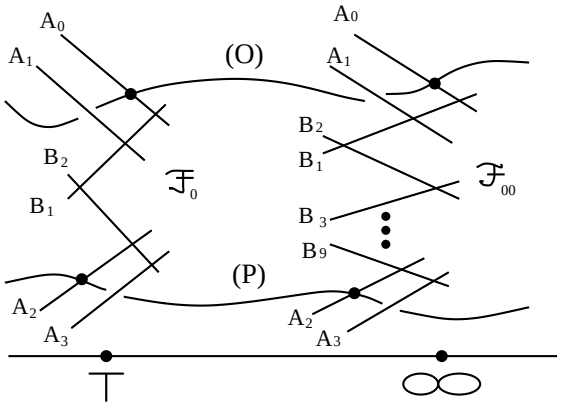


Figure 3: Intersections with special fibres

which is nonsingular at $u = v = 0$ (T is arbitrary). Computing the relative differential, we get

$$\frac{du}{1 + Tu + T^3u^2}$$

which is regular and non-zero on the affine part ($T \neq \infty$) restricted to O-section ($u = v = 0$).

For $T = \infty$, replace $T = 1/S$, the equation becomes

$$S^3v + S^2uv = S^3u^3 + u^2v + Suv^2$$

with relative differential

$$\frac{du}{1 + \frac{1}{S}u + \frac{1}{S^3}u^2}.$$

But now the equation itself is singular at $u = v = 0, S = 0$, so we have to desingularize by blowing up (twice as turns out). Finally, in the expression for the relative differential we substitute, as a result of blow-ups, $u = u'' \cdot S^2$

$$\frac{S^2du''}{1 + Su'' + Su''^2}$$

which is regular, and has a double-zero at $S = 0$. We conclude that the degree of $\Omega^1_{\mathcal{E}'/\mathbf{P^1}}|_O$ as a divisor is $2 \Longrightarrow$

$$(O)^2 = -2.$$

Also since the translation-by-P map

$$\tau_P \quad : \quad \mathcal{E}' \longrightarrow \mathcal{E}'$$

is an automorphism (for any P), c.f. [12] III.9.1, it follows $\tau_P^* D_1 \cdot \tau_P^* D_2 = D_1 \cdot D_2$ for any two divisors $D_1, D_2 \in Div(\mathcal{E}')$. Hence, $(P)\cdot(P) = \tau_P^*(P)\cdot\tau_P^*(P) = (O)\cdot(O) \Longrightarrow$

$$(P)^2 = -2.$$

Now we compute Φ_P in the definition of D_P. Let $\Phi_P = \sum_{i=0}^{3} a_i^0 A_i^0 + \sum_{i=1}^{2} b_i^0 B_i^0 + \sum_{i=0}^{3} a_i^\infty A_i^\infty + \sum_{i=1}^{9} b_i^\infty B_i^\infty = \Phi_P^0 + \Phi_P^\infty$. We have to find a_i's and b_i's, which reduces to solving two big systems of linear equations (for $\mathcal{F}_0$ and $\mathcal{F}_\infty$ separately). The first system is

$$\begin{cases} ((P)-(O)+\Phi_P^0)\cdot A_i^0 = 0 \quad i = 0,1,2,3 \\ ((P)-(O)+\Phi_P^0)\cdot B_i^0 = 0 \quad i = 1,2 \\ ((P)-(O)+\Phi_P^0)\cdot (O) = 0 \end{cases} \tag{8}$$

(P) intersects only A_2^0 and the intersection is 1, (O) intersects only A_0^0 and the intersection is 1 also. The last condition in (8) is to make the system solvable - it comes from the fact that Φ_P as it is defined is not unique, we can add the multiple of the whole fibre to it. The solution for (8) is the following:

$$a_0^0 = -2, \quad a_1^0 = -3/2, \quad a_2^0 = -3/4, \quad a_3^0 = -5/4, \quad b_1^0 = -3/2, \quad b_2^0 = -5/4$$

Similar computation for $\mathcal{F}_\infty$ gives $a_2^\infty = 1$ (to compute the height of (P) we actually need to know only the coefficients of the irreducible components through which it passes). Finally,

$$< P, P >= -D_P \cdot D_P \log q = -((P)-(O)+\Phi_P)\cdot((P)-(O)+\Phi_P)\log 2$$

$$= -D_P \cdot P \log 2 = -((P)^2 + \Phi_P \cdot P)\log 2 = -(-2-3/4+1)\log 2 = 7/4 \log 2. \tag{9}$$

Note that $P \cdot O = 0$, as they pass through distinct components in $\mathcal{F}_\infty$, and P has no poles on the affine part.

Now we can prove that $P = (T^3+T, T^3+T^2)$ is a generator for the infinite part of E' (see the previous section).

Let e be the l.c.m. of the exponents of the component groups of the fibres of E'. Assume for a moment that P and Q are arbitrary. Then $< eP, Q >= e < P, Q >$, but eP reduces to the same component as the identity at each place. Then the divisor $(eP)-(O)$ has zero intersection number with every fibre component and integer intersection with the O-section. After subtracting an integral multiple, say $f\cdot\mathcal{F}$, of the whole fibre we get our "corrected divisor" and

$$< P, Q > / \log q = -((eP)-(O)-f\mathcal{F})\cdot Q/e.$$

Since the intersection number is an integer, it follows that the denominator of $< P, Q > / \log q$ is bounded from above by e, for all P and Q.

In our case $e = 4 \Longrightarrow P$ is a generator, as if $P = nQ$ then

$$7/4 =< P, P > / \log 2 = n^2 < Q, Q > / \log 2 \quad \Longrightarrow \quad < Q, Q > / \log 2 = \frac{7}{4n^2},$$

and since 7 is square-free $n = 1$.

5 Equation for the Drinfeld modular curve of level $\Gamma_0(T^3)$

In this section we obtain an equation for the Drinfeld modular curve $X_0(T^3)$ as a smooth projective curve in $\mathbf{P}^2$. For the definition of Drinfeld modules, level structures, modular curves and etc. we refer to [3] and [5].

Let ϕ be a Drinfeld module of rank 2, i.e. a homomorphism

$$\phi : \quad A \longrightarrow F\{\tau\},$$

where τ is the Frobenius automorphism, $A = \mathbf{F}_2[T]$ and $F = \mathbf{F}_2(T)$. Rank 2 means $|a|_\infty^2 = \deg \phi(a)$.

A morphism between two Drinfeld modules $\phi \longrightarrow \phi'$ is $u \in F\{\tau\}$ such that $u\phi(a) = \phi'(a)u$, $\forall a \in A$. If $u \in F^\times$ this is an isomorphism.

Any rank 2 Drinfeld module $\phi : \ A \longrightarrow F\{\tau\}$ is uniquely determined by where it sends T, $\phi : \quad T \longrightarrow T + g\tau + \Delta\tau^2 = \phi_T$. We can normalize ϕ as follows: Let $\lambda \in F^\times$ and consider

$$\phi' : \ T \to \lambda\phi_T\lambda^{-1} = \lambda(T + g\tau + \Delta\tau^2)\lambda^{-1} = T + g\lambda^{1-q}\tau + \Delta\lambda^{1-q^2}\tau^2$$

since $q = 2$ we get $T + g\lambda^{-1}\tau + \Delta\lambda^{-3}\tau^2$, put $\lambda = g$ (assuming $g \neq 0$) then

$$\phi \cong \left(T \longrightarrow T + \tau + \Delta g^{-3}\tau^2\right).$$

Easy to see that two Drinfeld modules are isomorphic when $\frac{\Delta}{g^3} = \frac{\Delta'}{g'^3}$. Hence $j^{-1} = \Delta/g^3$ is an invariant of rank 2 Drinfeld modules (the inverse of the j-invariant). We choose to normalize by the inverse of the j-invariant since this simplifies the computations below. So Drinfeld modules are parametrized by the "j-line" $= \mathbf{P}^1$, as any of them can be written uniquely up to isomorphism as $T + \tau + z^{-1}\tau^2$. In particular, the modular curve of level 1, $X(1)$, is $\mathbf{P}^1$ with function field $F(\mathbf{P}^1) \cong F(z)$.

Since a nonsingular projective curve C over F is uniquely determined by its function field $F(C)$ we in fact will construct the function field of $X_0(T^3)$. In this situation morphisms of curves correspond to algebraic field extensions.

Using Drinfeld's definition of level, $F(X_1(T)) = F(a)$, where $\phi_T(a) = (T + \tau + z^{-1}\tau^2)(a) = 0$, i.e.

$$aT + a^2 + z^{-1}a^4 = 0$$
$$T + a + z^{-1}a^3 = 0.$$

Note that $z = a^3/(a+T)$, $a \in \overline{F(z)}$, and $X_0(T) = X_1(T)$. The idea of going up from $X_0(T)$ to $X_0(T^2)$, and from $X_0(T^2)$ to $X_0(T^3)$ resembles the Lubin-Tate construction of the torsion on formal groups.

$F(X_1(T^2))$ is $F(z, a, b)$ where

$$(T + \tau + z^{-1}\tau^2)(b) = a \qquad b \in \overline{F(z)}$$

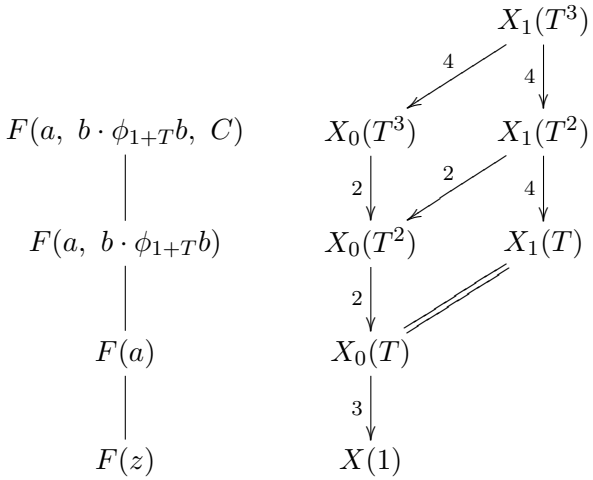
b is a generator of $\phi[T^2]$. As $(A/T^2)^\times =< 1, 1+T >$, b and $\phi_{1+T}(b)$ are two generators of the cyclic group $\phi[T^2]$. To construct $X_0(T^2)$ we want to remember the group but to forget the generators. So we form the symmetric combinations:

$$b + \phi_{1+T}(b) = b + b + \phi_T(b) = b + b + a = a$$

and

$$b \cdot \phi_T(b).$$

It follows that $X_0(T^2) = F(a, b \cdot \phi_{1+T}(b))$.



Let $B = b \cdot \phi_T(b) = b(b+a) = b^2 + ab$, also $Tb + b^2 + \frac{a+T}{a^3}b^4 = a$, so

$$a^3Tb + a^3b^2 + (a+T)b^4 = a^4 \tag{10}$$

We want to rewrite the last equation using only B, a and T.

$$b^4 = (b^2 + ab + ab)^2 = (b^2 + ab)^2 + a^2b^2 = B^2 + a^2b^2$$

Plug this into (10),

$$a^3Tb + a^3b^2 + (a+T)(B^2 + a^2b^2) = a^4$$
$$a^2T(ab + b^2) + (a+T)B^2 = a^4$$
$$a^2TB + (a+T)B^2 = a^4. \tag{11}$$

This is the equation of $X_0(T^2)$ with function field $F(a, B)$.

Do the same for $X_0(T^3)$. The strategy is the same, but the arithmetic is much more tedious.

Let $\phi_T(c) = b$, i.e.

$$Tc + c^2 + z^{-1}c^4 = b \tag{12}$$

$(A/T^3)^\times =< 1, 1+T, 1+T^2, 1+T+T^2 >$, and c, $\phi_{1+T}(c)$, $\phi_{1+T^2}(c)$, $\phi_{1+T+T^2}(c)$ are the generators of $\phi[T^3]$.

Next check that all symmetric combinations

$$c + \phi_{1+T}(c) + \phi_{1+T^2}(c) + \phi_{1+T+T^2}(c) = 0$$
$$c \cdot \phi_{1+T}(c) + c \cdot \phi_{1+T^2}(c) + \cdots + \phi_{1+T^2}(c) \cdot \phi_{1+T+T^2}(c) = b^2 + b^3 + b^4$$
$$c \cdot \phi_{1+T}(c) \cdot \phi_{1+T^2}(c) + \cdots + \phi_{1+T}(c) \cdot \phi_{1+T^2}(c) \cdot \phi_{1+T+T^2}(c) = b^4 + b^5$$

are in $F(a, B)$. We are left with

$$c \cdot \phi_{1+T}(c) \cdot \phi_{1+T^2}(c) \cdot \phi_{1+T+T^2}(c) = C$$

Now rewrite (12) using only C. After *long* computations one arrives at

$$C^2 + \frac{T(TB'^2 + TB' + 1)}{B'^5(TB' + 1)}C + \frac{(TB'^2 + TB' + 1)^8}{B'^{11}(TB' + 1)^2} = 0$$

where $B' = B/a^2$.

Let $C' = \frac{B'^6(TB'+1)^2}{(TB'^2+TB'+1)^4}C$, then

$$C'^2 + TB'C' + B'(TB' + 1)^2 = 0.$$

Finally, let $Y = T^2C'$ and $X = T^3B'$, then we get

$$Y^2 + TXY = X^3 + T^2X,$$

our original equation for E ! Thus

$$X_0(T^3) \cong E$$

and the modular parametrization turns out to be an isomorphism.

6 Heegner points from Drinfeld modular curves

Finally we are ready to compute explicitly the Heegner points on $X_0(T^3)$. For the definitions and the main properties of these points we refer to [1] and [10].

Let $U^2 + U = T$, and $K = F[U]$. K is an "imaginary" quadratic extension of F, i.e. ∞ does not split. This is easy to see from the Hurwitz genus formula $2g_K - 2 = 2(2g_F - 2) + R$. In this case $g_K = g_F = 0$ and $R \geq 0$ is the degree of ramification, and since nothing ramifies on the affine part it must be the infinity.

Note that T splits in K (and T is the only finite prime dividing the conductor of E). In this situation, we get a supply of points on $X_0(T^3)$, rational over the Hilbert Class Field of K (which in this case is K itself, as it is a UFD). Denote $\mathcal{O}_K := B$.

Consider a Drinfeld A-module of rank 2 with "CM" by B (i.e. $\mathrm{End}(\phi) = B$) with $\Gamma_0(T^3)$ structure, preserved by B. To construct them, start with a Drinfeld B-module of rank 1:

$$\widetilde{\phi}: \quad B \longrightarrow K\{\tau\}, \qquad \text{with } B/U^3 \cong A/T^3 \text{ structure.}$$

In general there are finitely many of these (in bijection with $\mathrm{Pic}(B)$), in our case there is only one:

$$\widetilde{\phi}: \quad U \longrightarrow U + \tau$$

Consider the composition

$$\phi: \quad A \hookrightarrow B \xrightarrow{\widetilde{\phi}} K\{\tau\}$$

We will get 2 possible ϕ depending on the choice of the ideal over T, but they will differ by some torsion when projected down to the elliptic curve.

Take

$$\begin{aligned} \phi_T = \widetilde{\phi}_U \cdot \widetilde{\phi}_{U+1} = (U+\tau)\cdot(U+1+\tau) \\ = U(U+1) + (U+U^2+1)\tau + \tau^2 = T + (1+T)\tau + \tau^2 \\ \cong \text{ (after normalizing) } T + \tau + (1+T)^{-3}\tau^2 \end{aligned}$$

To find the corresponding point on $X_0(T^3)$ one has to trace through the construction in the previous section with $z = (1+T)^3$. Then via the substitutions we made for $X_0(T^3) \cong E$ we get the Heegner point on $E(K) \cong E'(K)$. It turns out to be the generator P of the infinite part of $E'(F)$.

7 Birch and Swinnerton-Dyer conjecture and Gross-Zagier formula

In this section we combine our previous computations and directly verify Birch and Swinnerton-Dyer conjecture, as well as Gross-Zagier formula, for our curve E and its twist E'. Of course, the main purpose of Gross-Zagier formula is to prove BSD in certain cases but we will proceed in the reverse order. As a reference for these topics in function field situation the reader may consult [14], [7], [1], [10].

Recall that Birch and Swinnerton-Dyer conjecture (BSD) claims that if E is an elliptic curve over F (algebraic function field of transcendence degree one over a finite field k), then the order of vanishing of $L(E/F, s)$ at $s = 1$ is given by

$$\mathrm{ord}_{s=1} L(E/F, s) = \text{rank } E(F) = r \tag{13}$$

and moreover

$$\lim_{s\to 1} \frac{L(E/F, s)}{(s-1)^r} = \frac{\#III(E/F) \cdot \tau(E/F) \cdot \det < P_i, P_j >}{\#E(F)^2_{tor}} \tag{14}$$

where $III(E/F)$ is the Tate-Shafarevich group of E/F (which is conjectured to be finite), $\tau(E/F)$ is the Tamagawa measure of E/F and $\det < P_i, P_j >$ is the absolute value of the discriminant of the height pairing on E with respect to some basis of $E(F)$ modulo torsion.

Let $\mathcal{E}/k$ be the minimal proper regular model of E/F (in particular $\mathcal{E}/k$ is an elliptic surface). Tate in [14] proved that the *Tate conjecture* for $\mathcal{E}$ is equivalent to BSD for E. Moreover, in this case, Tate proved that (13) implies (14) up to a power of $p = \mathrm{char}\ F$. Extending this work Milne in [7] showed that the full refined conjecture is true at least if $p \neq 2$, and he removed the last assumption in [8] (Theorem 0.4(b) in [8] implies the main theorem in [7] and doesn't assume p is odd [1]).

Now we return to our example E and its twist E', and note that we know (13) for both E and E' from our previous explicit calculations. Hence, as was explained, we know also the refined version (14). For completeness we compute all the entries on the right hand-side of (14). Recall that (see [14], [13])

$$\tau = \prod_v c_v \cdot q^{-\deg(\Omega^1_{\mathcal{E}/C})|_O + 1 - g(C)}$$

where $c_v := \#E(F_v)/E_0(F_v)$ is the order of the subgroup of the component group which is rational over k_v. In our situation $C = \mathbf{P}^1$.

[1] I would like to thank J.S. Milne for explaining this to me

In section 2 we computed c_v's, and in section 4 we computed $\deg(\Omega^1_{\mathcal{E}'/\mathbf{P^1}})|_O = 2$. A similar calculation also shows that $\deg(\Omega^1_{\mathcal{E}/\mathbf{P^1}})|_O = 1$. Hence

$$\tau(E/F) = 4 \cdot 4 \cdot 2^{-1+1} = 16 \qquad \text{and} \qquad \tau(E'/F) = 4 \cdot 4 \cdot 2^{-2+1} = 8.$$

Next, since $\mathrm{rank}E(F) = 0$, the regulator $R_E = \det < P_i, P_j >= 1$, and as we computed in section 4, $R_{E'} =< P, P >= \frac{7}{4}\log 2$. Also $L(E/F, 1) = 1$, $L'(E'/F, 1) = \frac{7}{2}\log 2$ from section 3. Hence we deduce from (14) that $\#III(E/F) = \#III(E'/F) = 1$.

We briefly sketch an alternative approach to computing the order of Tate-Shafarevich group which relies only on Tate's original result [14].

Since for our curves E and E' we know (13) and can compute all the entries in (14) except $\#III$, from Tate's results in [14] we deduce $III_\ell = 1$ for $\ell \neq 2$. Hence it is enough to prove that $III_2 = 1$. To do this one can use the exact sequence

$$0 \longrightarrow E(F)/2E(F) \longrightarrow Sel(F, 2) \longrightarrow III_2 \longrightarrow 0$$

and 2-descent [15]. Here $Sel(F, 2)$ is the Selmer group of the isogeny induced by multiplication by 2 on E (the cohomology groups are in fppf topology, loc. cit.). So it is enough to compute $Sel(F, 2)$, and since $Sel(F, 2)$ is defined to be the set of elements in $H^1(F, \ker 2)$ whose restrictions to $H^1(F_v, \ker 2)$ lie in $Sel_v(F, 2)$ for all v, it is enough to compute $Sel_v(F, 2)$. But there is another exact sequence of local Selmer groups

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow Sel_v(F, Frob) \longrightarrow Sel_v(F, 2) \longrightarrow Sel_v(F, Ver) \longrightarrow 0$$

and hence one is reduced to computing $Sel_v(F, Frob)$ and $Sel_v(F, Ver)$. Proposition 3.1 in [15] describes large portions of these groups, and the rest can be deduced using Tate's duality and explicit 2-descent (6.1) *loc.cit.*, c.f. also Example(8.1) in *loc.cit.*

Now we turn to verifying the Gross–Zagier formula in function field setting. When characteristic is *odd* Rück and Tipp [10] have proved the following analogue

$$\frac{\partial}{\partial s}\left(L(E/K, s)\right)|_{s=1} = \frac{\partial}{\partial s}\left(L(E/F, s)L(E'/F, s)\right)|_{s=1} \tag{15}$$

$$=< P, P >_K \cdot c(D) \cdot (\deg \wp)^{-1} \int_{\Gamma_0(N)\backslash GL_2(K_\infty)/\Gamma_\infty K_\infty^\times} f \cdot \bar{f}$$

where $K = F(\sqrt{D})$ is an imaginary quadratic extension, E' is the quadratic twist of E by K, $< P, P >_K$ is the canonical height of the Heegner point computed over K, $\deg \wp$ is the degree of the modular parametrization $X_0(N) \longrightarrow E$, $c(D)$ equals $\frac{q-1}{2}q^{-(\deg D+1)/2}$ (if $\deg D$ is odd) or $\frac{q-1}{4}q^{-(\deg D)/2}$ (if $\deg D$ is even), and finally the last entry on the right is the Petersson inner

product (f, f) of the newform associated to E (note that this theorem applies to *all* elliptic curves with split multiplicative reduction at ∞ by (1.1)).

Even though the proof of (15) assumes that the characteristic is odd, our computations will very nicely match this formula. First we need to define the Petersson inner product. (A good reference for whatever follows below is [5]; actually the Petersson inner product for our example is calculated in (9.7.3) of [5] but we will sketch how it is done).

As before let $A = \mathbf{F}_q[T]$, $F = \mathbf{F}_q(T)$. Also take $\pi = T^{-1}$ to be the uniformizer at infinity, and $F_\infty = \mathbf{F}_q((\pi))$, $\mathcal{O}_\infty = \mathbf{F}_q[[\pi]]$ ∞-adic integers.

Denote $\mathcal{K} = GL_2(\mathcal{O}_\infty)$, and $\mathcal{I} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{K} | c \equiv 0 (\mod \pi) \right\}$ the Iwahori subgroup. If $\mathcal{T}$ is the Bruhat-Tits tree of $PGL_2(K_\infty)$ then vertices $X(\mathcal{T})$ and oriented edges $Y(\mathcal{T})$ are isomorphic to

$$X(\mathcal{T}) \cong GL_2(F_\infty)/\mathcal{K} \cdot F_\infty^*$$

$$Y(\mathcal{T}) \cong GL_2(F_\infty)/\mathcal{I} \cdot F_\infty^*$$

Denote $o(e)$, $t(e)$, $\bar{e}$ the origin, terminus and the inverse of an edge e.

Consider the following conditions on $\mathbf{C}$-valued functions f on $Y(\mathcal{T})$:

(i) $f(e) + f(\bar{e}) = 0 \qquad \forall e \in Y(\mathcal{T})$

(ii) $\sum_{\substack{e \in Y(\mathcal{T}) \\ t(e) = v}} f(e) = 0 \qquad \forall v \in X(\mathcal{T})$

(iii) $f(\gamma e) = f(e) \qquad \forall e \in Y(\mathcal{T}), \quad \forall \gamma \in \Gamma_0(N)$

(iv) f has compact (=finite) support modulo $\Gamma_0(N)$ (this means that f vanishes eventually on each of the half-lines (=cusps) of $\Gamma_0(N) \setminus \mathcal{T}$.)

Functions satisfying (i)-(iv) are called *automorphic cusp forms of level* N (of Jacquet-Langlands-Drinfeld type), [5]. Denote them by $H_!(\mathcal{T}, \mathbf{C})^{\Gamma_0(N)}$. They carry the role of cusp forms of weight 2 in the classical setting.

Let C be the completed algebraic closure of F_∞. The function field analogue of the upper-half plane is the *Drinfeld upper-half plane*

$$\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(F_\infty) = C - F_\infty$$

It has a natural structure of a rigid analytic space over F_∞. Drinfeld proved that there exists a smooth affine algebraic curve $Y_0(N)$ defined over F such that $\Gamma_0(N) \setminus \Omega$ is isomorphic, as an

analytic space, to the analytification $Y_0(N)^{an}$ of $Y_0(N)$. The *Drinfeld modular curve* (of level N) $X_0(N)$ is the smooth projective model of $Y_0(N)$.

$$X_0(N) = \Gamma_0(N) \setminus \Omega \cup \{\text{cusps}\}$$

Let $J_0(N)$ denote the Jacobian variety of $X_0(N)$. A refined version of (1.1) states that there is a canonical bijection between the sets of

a) normalized Hecke eigenforms f in $H_!^{new}(\mathcal{T}, \mathbf{Q})^{\Gamma_0(N)}$ with rational eigenvalues

b) one-dimensional isogeny factors of $J_0^{new}(N)$

c) isogeny classes of elliptic curves E/K with conductor $N_E = N \cdot \infty$, and with split multiplicative reduction at ∞

"New" here has the same meaning as over $\mathbf{Q}$, with $H_!$ being replaced by the space of cusp forms of weight 2. For details see [5]. Moreover the relation between L-functions of corresponding f and E is

$$L(E, s) = L(f, s)$$

Hence for any elliptic curve E over K with split multiplicative reduction at ∞ and conductor $N \cdot \infty$ there is a non-trivial morphism

$$\wp \ : \quad X_0(N) \longrightarrow E.$$

To determine the newform corresponding to the elliptic curve one needs to examine the analytic reduction of $X_0(N)$, regarded as a rigid analytic space, which is isomorphism to $\Gamma_0(N) \setminus \mathcal{T}$.

$\Gamma := GL_2(F_\infty)$ acts on $\mathcal{T}$ in an obvious way. Inversion is given by multiplication on the right by $\begin{pmatrix} 0 & 1 \\ T^{-1} & 0 \end{pmatrix}$.

$\Gamma_0(N)$ is a discrete subgroup in Γ and we need to analyze $\Gamma_0(N) \setminus \mathcal{T}$. There are two canonical maps $X(\mathcal{T}) \longrightarrow Y(\mathcal{T})$, which associate to each oriented edge e_i its origin $o(e_i)$ or terminus $t(e_i)$. For each $i \in \mathbf{Z}$, let v_i (resp. e_i) be the vertex (resp. edge) represented by the matrix $\begin{pmatrix} T^i & 0 \\ 0 & 1 \end{pmatrix}$, then $o(e_i) = v_i$, $t(e_i) = v_{i+1}$.

Theorem 7.1 (Weil, c.f. [4]) *The subgraph of $\mathcal{T}$ formed by v_i and e_i with $i \geq 0$ is a fundamental domain for Γ, i.e. maps isomorphically onto the quotient graph $\Gamma \setminus \mathcal{T}$.*

One constructs $\Gamma_0(N) \setminus \mathcal{T}$ by examining the "ramified covering"

$$\varphi \ : \quad \Gamma_0(N) \setminus \mathcal{T} \longrightarrow \Gamma \setminus \mathcal{T}$$

It suffices to know the edges e of $\Gamma_0(N) \setminus \mathcal{T}$ oriented such that $\varphi(e) = e_i$, some i. Let

$$X_i = \{v \in X\left(\Gamma_0(N) \setminus \mathcal{T}\right) \mid \varphi(v) = v_i\}$$

be the vertices of type i, and similarly

$$Y_i = \{e \in Y\left(\Gamma_0(N) \setminus \mathcal{T}\right) \mid \varphi(e) = e_i\}$$

be the edges of type i. Put

$$G_0 = GL_2(\mathbf{F}_q) \quad , \quad G_i = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma \mid \deg b \leq i\}, \quad i \geq 1$$

G_i is the stabilizer of v_i in Γ and $G_i \cap G_{i+1}$ is the stabilizer of e_i. Hence

$$G_i \setminus \Gamma / \Gamma_0(N) \cong X_i(\Gamma_0(N) \setminus \mathcal{T})$$

$$G_i \cap G_{i+1} \setminus \Gamma / \Gamma_0(N) \cong Y_i(\Gamma_0(N) \setminus \mathcal{T})$$

One has the following easy

Lemma 7.2

$$\Gamma / \Gamma_0(N) \cong \mathbf{P}^1(\mathbf{F}_q[T]/N)$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow (a : c)$$

as $GL_2(\mathbf{F}_q[T])$-sets.

So finally, the problem reduces to finding the orbits of G_i acting on $\mathbf{P}^1(\mathbf{F}_q[T]/N)$.

Let $\deg N = d$. Then orbits of $G_{d-1}, G_d, G_{d+1}, \ldots$ are the same, or in other words the subgraph of $\Gamma_0(N) \setminus \mathcal{T}$ consisting of the edges of type $\geq d-1$ is a disjoint union of $X_{d-1}(\Gamma_0(N) \setminus \mathcal{T})$ half-lines, and these are the cusps.

Returning to our example: $N = T^3$ and $q = 2$. In this situation one easily computes that X_0 consists of the orbit of $(T : 1)$, X_1 has two elements represented by the orbits of $(0 : 1)$) and $(T^2 : 1)$, and finally that X_2 has one element represented by the orbit of $(0 : 1)$. Moreover all these 4 vertices are cusps (i.e. there are infinite half-lines attached to them), and the edges join these four vertices into a rectangle (see the figure)

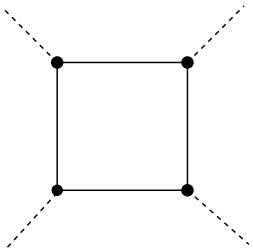


Figure 4: $\Gamma_0(T^3) \setminus \mathcal{T}$

Now it is clear that essentially there is only one automorphic cusp form on $\Gamma_0(T^3) \setminus \mathcal{T}$: the one which maps every clockwise oriented edge of the square to 1, and is zero on the half-lines (the cusps).

Once we know $\Gamma_0(T^3) \setminus \mathcal{T}$ and the cusp form, we can compute the Petersson inner product on $H_!(\mathcal{T}, \mathbf{Z})^{\Gamma_0(T^3)} \cong \mathbf{Z}f$ which enters the Gross-Zagier formula.

The volume $\mu(e)$ of each edge is 1,

$$(f, f) = \sum_{e \in Y(\Gamma_0(T^3) \setminus \mathcal{T})} f(e) \cdot f(e) \mu(e) = 4.$$

Finally we are ready to calculate the quantities entering the Gross–Zagier formula (15). Left hand-side is equal to $L'(E'/F, 1) = \frac{7}{2} \log 2$ by section 3. A computation very similar to the one in section 4 gives $< P, P >_K = \frac{7}{2} \log 2$; $\deg \wp = 1$ for the trivial reason $E \cong X_0(T^3)$, and finally from above $(f, f) = 4$.

So we see that the constant $c(T)$ is equal to $1/4$, which is exactly $\frac{q-1}{2} q^{-(\deg T + 1)/2}$ except that one replaces the Kummer extension $F(\sqrt{D})$ by the Artin–Schreier extension $F(U)$, $U^2 + U = T$.

8 Analytic computation of Heegner points

In this last section we present an alternative approach to the computation of Heegner points using rigid analytic theta series. This approach is more suitable in general than the one we used before as the equations of Drinfeld modular curves become very complicated when the level is large. A reference for this section is [5].

First we recall the main result in [5]. Let E be an optimal elliptic curve with split multiplicative reduction at ∞ and conductor $N \cdot \infty$, and let

$$\wp \ : \qquad X_0(N) \longrightarrow E$$

be the modular parametrization. E.-U. Gekeler and M. Reversat came up with an explicit description of $\wp$.

Let $\widetilde{\Gamma_0(N)} := \Gamma_0(N)/(K_\infty^* \cap \Gamma_0(N))$, and let $\overline{\Gamma} := \Gamma_0(N)^{ab}/(\Gamma_0(N)^{ab})_{tor}$ be the maximal torsion-free abelian quotient of $\Gamma_0(N)$. Let $\omega \in \Omega$ be an arbitrary base point and $\alpha \in \Gamma_0(N)$. Put

$$u_\alpha(z) = \prod_{\gamma \in \widetilde{\Gamma_0(N)}} \left(\frac{z - \gamma\omega}{z - \gamma\alpha\omega} \right)$$

Then one can show that $u_\alpha(z)$ converges locally uniformly to an invertible function u_α on Ω that does not depend on the choice of $\omega \in \Omega$, and depends only on the class of $\overline{\alpha}$ of α in $\overline{\Gamma}$.

Also one can show [4] that there is a canonical isomorphism

$$i \ : \quad \overline{\Gamma} \cong H_!(\mathcal{T}, \mathbf{Z})^{\Gamma_0(N)}$$

Let $f \in H_!^{new}(\mathcal{T}, \mathbf{Z})^{\Gamma_0(N)}$ with rational eigenvalues which is primitive (i.e. $f \notin nH_!(\mathcal{T}, \mathbf{Z})^{\Gamma_0(N)}$ for $n > 1$). Write f also for a representative of its preimage $i^{-1}(f) \in \overline{\Gamma}$ in $\Gamma_0(N)$.

Gekeler-Reversat theorem is summarized in the following commutative diagram:

$$\begin{array}{ccccc}
\Omega & & \xrightarrow{\quad u_f \quad} & & C^* \\
\downarrow & & & & \downarrow \\
\Gamma_0(N) \setminus \Omega & & & & C^*/q^{\mathbf{Z}} \\
\| & & & & \| \\
Y_0(N)(C) & \hookrightarrow & X_0(N)(C) & \xrightarrow{\wp} & E_f(C)
\end{array}$$

where q is the Tate period, and E_f is the optimal curve for f.

Remark For our purposes $u_f(z)$ will be essentially the analogue of $\int_{i\infty}^z f(s)ds$, with f a newform for $E/\mathbf{Q}$.

To apply Gekeler-Reversat formula we need to find a representative of the generator of the cyclic group $\overline{\Gamma} := \Gamma_0(T^3)^{ab}/(\Gamma_0(T^3)^{ab})_{tor}$ in $\Gamma_0(T^3)$.

$GL_2(\mathbf{F}_2[T])$ is generated by

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad T_0 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \dots \ , \ T_n = \begin{pmatrix} 1 & 0 \\ T^n & 1 \end{pmatrix}, \ \dots$$

Note that all these elements are torsion.

Chose an element $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL_2(\mathbf{F}_2[T])$ which is in $\Gamma_0(T^3)$, non-torsion, and the maximum of the degree of its nonzero entrees is 3 (as low as possible), e.g.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ T^3 & 1 \end{pmatrix} = \begin{pmatrix} 1+T^3 & 1 \\ T^3 & 1 \end{pmatrix}.$$

This will be a possible representative of f we need.

Now using Drinfeld's theorem on the equivalence of categories of rank-2 Drinfeld A-modules over C and homothety classes of rank-2 A-lattices, to compute the Heegner point we need to compute

$$u_f(U)$$

where $U^2 + U = T$ (i.e. we pick an A-lattice having complex multiplication by $A[U]$, namely $A \bigoplus UA$, and use the commutativity of the Gekeler-Reversat diagram).

To be able to approximate the infinite product

$$u_f(U) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{U - \gamma\omega}{U - \gamma\eta}$$

one has to know how fast it converges in C. So assume ω and z are fixed, and since ω can be arbitrary take it to be equal to U. This considerably simplifies the actual computations since then we are dealing with a quadratic extension.

$$\left|\frac{z - \gamma\omega}{z - \gamma\eta} - 1\right| = \frac{|\det\gamma||\eta - \omega|}{|z - \gamma\eta||c\eta + d||c\omega + d|} = \frac{|\eta - \omega|}{|z - \gamma\eta||c\eta + d||c\omega + d|} =$$

$$= \frac{|\eta - \omega|}{|z(c\eta + d) - (a\eta + b)||c\omega + d|}$$

where the norms are the ∞-adic norms. Substitute $z = U$, $\omega = U$ to get

$$\frac{|\eta - \omega|}{|U(c\eta + d) - (a\eta + b)||cU + d|}$$

Put $\deg(0) = 0$. Since U is not in $\mathbf{F}_2[T]$ $\deg(cU + d) \geq \max(\deg(c), \deg(d))$. Hence $|cU + d| \geq \max(|c|, |d|)$.

With our choice of ω, $\eta = \frac{(1+T^3)U+1}{T^3U+1}$. Substituting this into $|U(c\eta + d) - (a\eta + b)|$ one can easily show that $|U(c\eta + d) - (a\eta + b)| \geq \text{const } |b|$. So finally,

$$\left|\frac{z - \gamma\omega}{z - \gamma\eta} - 1\right| \leq \frac{\text{const}}{|b| \cdot \max(|c|, |d|)}$$

and the constant doesn't depend on γ.

Also since $ad - cb = 1$, $\deg(a) \leq \max(\deg(b), \deg(c), \deg(d)) \Longrightarrow |a| \leq \max(|b|, |c|, |d|) \Longrightarrow |b| \cdot \max(|c|, |d|) \geq \max(|a|, |b|, |c|, |d|)$, and

$$\left|\frac{U - \gamma U}{U - \gamma\eta} - 1\right| \leq \frac{\text{const}}{\max(|a|, |b|, |c|, |d|)}$$

This suggests that to compute $u_f(U)$ with good accuracy one can take a finite product over the matrices in $\Gamma_0(T^3)$ with entries having degree less than some N. The following crude estimates show that N need not be large.

Let $T(N)$ be the number of matrices in $\Gamma_0(N)$ with $\ell := \max \deg(a,b,c,d) = N$. Since $T(N) \ll q^N$

$$\prod_{\gamma\in\Gamma_0(n),\ \ell\geq N}\left|\frac{z-\gamma\omega}{z-\gamma\eta}\right| \leq \prod_{k\geq N}\left(1+\frac{1}{q^k}\right)^{T(k)} \asymp O\left(\prod_{k\geq N}\left(1+\frac{1}{q^k}\right)\right) = O(e^{1/q^N})$$

With $N=5$, we get the following ∞-adic approximation of the Heegner point

$$u = \prod_{\gamma\in\Gamma_0(T^3),\ \ell\leq 5,\ \gamma\neq 1,\gamma\neq f^{-1}} \frac{U-\gamma U}{U-\gamma\begin{pmatrix}1+T^3 & 1\\ T^3 & 1\end{pmatrix}U} = \frac{LU+M}{D}$$

Product has 1641 terms and $L, M, D \in \mathbf{F}_2[T]$ with

$$L = T^{83112}+T^{83111}+T^{83105}+T^{83104}+T^{83102}+T^{83101}+T^{83100}+T^{83097}+T^{83094}+T^{83089}+\cdots$$

$$M = T^{83109}+T^{83108}+T^{83107}+T^{83105}+T^{83104}+T^{83099}+T^{83097}+T^{83094}+T^{83093}+T^{83090}+\cdots$$

$$D = T^{77498}+T^{77497}+T^{77496}+T^{77494}+T^{77490}+T^{77488}+T^{77486}+T^{77484}+T^{77483}+T^{77482}+\cdots$$

Finally we need to map this point to our elliptic curve $E\ :\ Y^2+TXY = X^3+T^2X$, i.e. to pass from the Tate curve to the curve in Weierstrass form. This can be done using Tate's theorem [12] V.3.1.

To apply the theorem first convert E to the suitable form given in V.3.1(a) *loc.cit.* by substituting $X = T^2X'$, $Y = T^3Y' + T$ to get

$$E \cong E_q\ :\quad Y^2+XY = X^3+1/T^4.$$

Now in this form the generator of the infinite part of $E_q(K)$ is given by

$$P = (T^5+T^3, T^3(T^3+T+(U^3+U)(T^3+T))+T)$$

(which as we saw is also the Heegner point).

A fact which considerably simplifies the calculations is the following: as one easily verifies

$$|x([n]P)| \sim |x(P)|^n.$$

$E_q(K)$ has small torsion which doesn't affect the overall distribution of its points, and one checks that to determine the x-coordinate of a point on $E_q(K)$ it is enough to approximate it within 2^{-3}, i.e. if $|x(Q_1)-x(Q_2)| < 2^{-3}$ and $Q_1, Q_2 \in E_q(K)$ then $x(Q_1) = x(Q_2)$. The later verification can be done, for example, using the continuous fractions algorithm.

We will verify that under Tate's map

$$C/q^{\mathbf{Z}} \longrightarrow E_q \tag{16}$$

$$u \longrightarrow (X(u,q), Y(u,q)) \tag{17}$$

$X(u,q)$ approximates $x(P)$.

The only thing which is still missing is the Tate period q of E_q. But since we know the j-invariant of E_q we can take a short-cut (i.e. avoid using theta functions for this): We know $j(E_q) = T^4$, and by [12] V. Lemma 5.1 one has

$$\frac{1}{j(E_q)} = q - 744q^2 + 356652q^3 - \cdots \in \mathbf{Z}[[q]]$$

As the first few coefficients in $g(q)$ are even and the distribution of points of $E_q(K)$ is sparse we can take $q_E \asymp \frac{1}{T^4}$.

Now in characteristic 2 the infinite sum for $X(u,q)$ V.3.1(c) *loc.cit.* is given by

$$X(u,q) = \frac{u}{1-u^2} + \sum_{n\geq 1}\left(\frac{q^n u}{1-q^{2n}u^2} + \frac{q^n u^{-1}}{1-q^{2n}u^{-2}}\right)$$

With our q and u one verifies that to get the value of $X(u,q)$ within 2^{-3} accuracy it is enough to sum up the first 1500 terms. Again a computer calculation shows that the ∞-adic absolute value of $X(u,q)$ approximates $|x(P)|$. This concludes our calculations.

References

[1] M. Brown, *On a conjecture of Tate for elliptic surfaces over finite fields*, Proc. London Math. Soc. **69** (1994), 489–514.

[2] B. Gross, *Kolyvagin's work on modular elliptic curves*, London Math. Soc. Lecture Note Ser. **153** (1991), 235–256.

[3] E.-U. Gekeler, *Drinfeld modular curves*, Springer, LNM **1231** (1986)

[4] E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Internat. J. Math. **6**, (1995), 689–708.

[5] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine angrew. Math. **476** (1996), 27–93.

[6] R. Hartshorne, *Algebraic geometry*, Springer, GTM **52** (1977)

[7] J. S. Milne, *On a conjecture of Artin and Tate*, Annals of Math. **102** (1975), 517–533.

[8] J. S. Milne, *Values of zeta functions of varieties over finite fields*, Amer. J. of Math. **108** (1986), 297–360.

[9] M. Reversat, *Sur les revêtements de Schottky des courbes modulaires de Drinfeld*, Arch. Math. **66** (1996), 378-387.

[10] H.-G. Rück and U. Tipp, *Heegner points and L-series of automorphic cusp forms of Drinfeld type*, Documenta Math. **5** (2000), 365–444.

[11] J. Silverman, *The arithmetic of elliptic curves*, Springer, GTM **106** (1986).

[12] J. Silverman, *Advanced topics in the arithmetics of elliptic curves*, Springer, GTM **151** (1994).

[13] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, LNM **476** (1975), 33–52.

[14] J. Tate, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki **9**, Soc. Math. France, Paris (1966), Exp. No. 306, 415–440.

[15] D. Ulmer, *p-descent in characteristic p*, Duke Math. J. **62** (1991), no. 2, 237–265.