Computation of Heegner Points for Function Fields

Abstract

This is a write-up of the project done under the direction of Douglas Ulmer at Arizona Winter School 2000. We carefully explain how to compute explicitly the Heegner points for an elliptic curve defined over $\mathbf{F}_2(T)$.

1 Introduction

This is a preliminary version.

These are the notes[1] of the project done under the direction of Douglas Ulmer at Arizona Winter School 2000 - *The Arithmetic of Function Fields.*

The goal was to compute the quantities showing up in the Gross-Zagier formula for function fields for one concrete example. 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 [4] 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 [4] 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 [5].

Now let F be the function field of a smooth projective curve over a finite field. Choose some place ∞ of F to be the place at "infinity". Let E be an elliptic curve defined over F with split multiplicative reduction at ∞, K be an imaginary quadratic extension in which all primes dividing the conductor of E (except ∞) split, and $P_K \in E(K)$ be the Heegner point defined via the modular parametrization $X_0(n) \longrightarrow E$. Then

[1]Notes by Mihran Papikian; papikian@umich.edu

Theorem 1.1 (Gross-Zagier formula for function fields) *The height $< P_K, P_K >$ of P_K satisfies*

$$< P_K, P_K >= c \cdot L'(E/K, 1)$$

where c is a nonzero constant, and $L'(E/K, 1)$ is the value of the first derivative of L-functions of E/K at 1.

The non-zero constant c depends on the normalization of the measure in the Petersson inner product.

In particular, if $L'(E/K, 1) \neq 0$, then $\mathrm{rank} E(K) \geq 1$ and the Birch and Swinnerton-Dyer conjecture holds for E over K, using the results of Tate and Milne [9]. To prove BSD for E over F one has to use non-vanishing theorems of twists of $L-$functions.

D. Ulmer announced the proof of (1.1) in the case of an arbitrary function field F at Arizona Winter School 2000. Earlier, Rück and Tipp announced a similar result for $F = \mathbf{F}_q(T)$, their paper appeared recently [6].

One should observe that Kolyvagin type argument is redundant for function fields once (1.1) is true, as here $\mathrm{rank} E(K) \leq \mathrm{ord}_{s \to 1} L(E/K, s)$ and if $\mathrm{ord}_{s \to 1} L(E/K, s) = 1$ then Heegner point is of infinite order $\Longrightarrow \mathrm{rank} E(K) \geq 1 \Longrightarrow$ equality holds $\Longrightarrow$ BSD follows from the work of Tate and Milne.

M. Brown in [1] proves for $F = \mathbf{F}_q(T)$, using Euler systems of Heegner points, that if P_K is non-torsion then $\mathrm{rank} E(K) = 1$. The paper very closely follows the argument given in Gross, [2].

The constant c in (1.1) depends on the normalization of the measure in Petersson inner product.

Let now $F = \mathbf{F}_2(T)$ be the rational function field in one variable over $\mathbf{F}_2$, and consider the elliptic curve E over F with affine equation

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

and its quadratic twist E' with affine equation

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

The quadratic extension is $K = F(U)$ where $U^2 + U = T$. The isomorphism between E and E' are 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.

2 Elementary Invariants

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

One easily computes $\Delta = T^8$, and $j = T^4$. It has a cuspidal reduction at $T = 0$. Tate's algorithm [8] shows that the reduction type is I_1^* in Kodaira's notation, i.e. this fibre has 6 irreducible components in the Neron model, four of which occur with multiplicity one. Component group is $\mathbf{Z}/4$. 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

$$\mathrm{cond}(E) = T^3 \cdot \infty.$$

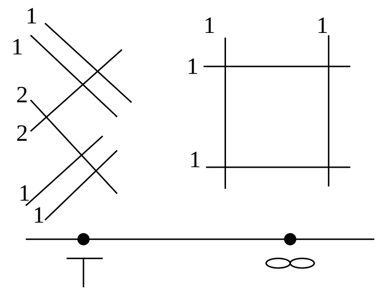

Figure 1: Special fibres on E

Similarly for

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

$\Delta = T^8$, 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 $\mathbf{Z}/4$. 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 $\mathbf{Z}/2 \times \mathbf{Z}/2$, and ∞ in the conductor occurs with degree 4.

Finally, the conductor of E' is

$$\mathrm{cond}(E') = T^3 \cdot \infty^4.$$

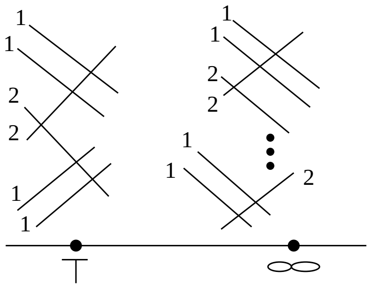

Figure 2: Special fibres on E'

3 Computing the L-functions

Since E and E' are non-constant over F, the L-functions of E and E' are polynomials in q^{-s} of degree = degree of the conductor - 4 (by Grothendieck). For E conductor is $T^3 \cdot \infty \Longrightarrow L$ has degree 4-4=0 $\Longrightarrow$

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

From Tate's geometric version of BSD [9], $\mathrm{rank}(E) \leq \mathrm{ord}L(E/F, 1)$, this gives, in our example, $\mathrm{rank}(E)$=0.

For E' conductor is $T^3 \cdot \infty^4 \Longrightarrow L$ has degree 7-4=3.

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

where $q = 2$.

To compute c_i's one can either compute enough of the local factors (for places up to degree 3), or alternatively can use the functional equation (sign is "-" as rank of E' turns out to be 1), and compute the local factors up to degree 1 (only one place in this case!).

$$L(E'/F, s) = \prod_v L_v(q_v^{-s})^{-1}, \qquad q_v = 2^{\deg v}$$

where

$$L_v(q_v^{-s}) = \begin{cases} 1 - a_v q_v^{-s} + q_v q_v^{-2s} & \text{good reduction,} \\ 1 - q_v^{-s} & \text{split multiplicative,} \\ 1 + q_v^{-s} & \text{non-split multiplicative,} \\ 1 & \text{additive.} \end{cases} \tag{5}$$

and

$$a_v = q_v + 1 - \sharp \widetilde{E}'(k_v).$$

At $v = T$, E' has additive reduction so the local factor is 1. At $1+T$, $\sharp \widetilde{E}'(k_{T+1}) = 2$, similarly $\sharp \widetilde{E}'(k_{1+T+T^2}) = 6$, $\sharp \widetilde{E}'(k_{1+T^2+T^3}) = 10$, $\sharp \widetilde{E}'(k_{1+T+T^3}) = 12$.

This is enough to compute the L-function without any assumptions, put $\lambda = 2^{-s}$

$$L(E'/F, s) = \frac{1}{1 - \lambda + 2\lambda^2} \cdot \frac{1}{1 + \lambda^2 + 4\lambda^4} \cdot \frac{1}{1 + \lambda^3 + \cdots} \cdot \frac{1}{1 + 3\lambda^3 + \cdots} \cdots$$
$$= 1 + 2^{-s} - 2 \cdot 2^{-2s} - 8 \cdot 2^{-3s} + 0 + 0 \cdots.$$

The alternative approach using the functional equation,

$$\Lambda(E'/F, s) := |\text{conductor}|^{-s/2} |d_F|^{-s} L(E'/F, s) = \pm \Lambda(E'/F, 2 - s)$$

The conductor is of degree 7 $\implies$ $|\text{conductor}| = 2^{-7}$, d_F is the discriminant of F, $|d_F| = 2^{2-2\text{genus}} = 2^2$ in our case. The sign is '-'.

From computing only $\sharp \widetilde{E}'(k_{T+1}) = 2$, we know

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

The functional equation yields

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

from which it follows that $c_2 = -2$ and $c_3 = -8$. So

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

Now $L(E'/F, 1) = 0$, but $L'(E'/F, 1) = 7/2 \log 2$. Again by Tate

$$\text{rank}(E') \leq 1$$

4 E and E' as groups

From L-function computations we know that $E: Y^2+TXY = X^3+T^2X$ is torsion over $F = \mathbf{F}_2(T)$.

First 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

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

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'.

5 Computing the height pairing

$P = (T^3+T, T^3+T^2)$ 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 the Neron model $\mathcal{E}'$.

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,

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

So

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

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

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

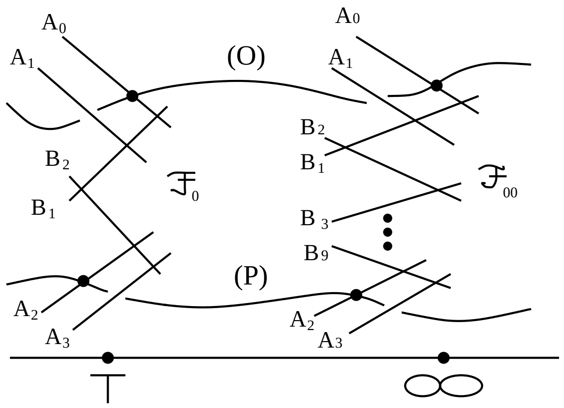

Figure 3: Intersections with special fibres

For our computations we will also need the self-intersection of $(O) \cdot (O)$. Using the adjunction formula,

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

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

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

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 $u = u'' \cdot S^2$ as a result of blow-ups

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

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), 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, $(P) \cdot (P) = \tau_P^*(P) \cdot \tau_P^*(P) = (O) \cdot (O) \Longrightarrow$

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

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 [7] is the following

$$< P, P >= -D_P \cdot D_P \log q$$

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

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

$$\begin{cases} ((P) - (O) + \Phi_P^0) \cdot A_i^0 = 0 & i = 0, 1, 2, 3 \\ ((P) - (O) + \Phi_P^0) \cdot B_i^0 = 0 & i = 1, 2 \\ ((P) - (O) + \Phi_P^0) \cdot (O) = 0 & \end{cases} \tag{6}$$

(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 (6) 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 whole fibre to it. The solution for (6) 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,

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

$$-D_P \cdot P \log 2 = -((P)^2 + \Phi_P \cdot P) \log 2 = -(-2 - 3/4 + 1) \log 2 = 7/4 \log 2$$

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'.

Let e be the lcm 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 by e, for all P and Q.

In our case $e = 4 \Longrightarrow P$ is a generator, as if $P = nQ$ then $7/4 =< P, P > / \log 2 = n^2 < Q, Q > / \log 2 \Longrightarrow < Q, Q > / \log 2 = \frac{7}{4n^2}$, and since 7 is square-free $n = 1$.

6 Birch and Swinnerton-Dyer formula

In our case the formula (conjecture) states

$$L'(E'/F, 1) = \frac{\sharp III(E'/F) \cdot < P, P > \cdot \tau}{\sharp E'(F)^2_{tor}}$$

where τ is the Tamagawa number. At this point we can compute all the entries except III.

$$\tau = \prod_v \sharp E'(F_v)/E'_0(F_v) \cdot q^{-\deg(\Omega^1_{\mathcal{E}'/\mathbf{P}^1})|_O + 1 - g} = 4 \cdot 4 \cdot 2^{-2+1} = 8$$

$$7/2 \log 2 = \frac{\sharp III(E'/F) \cdot 7/4 \log 2 \cdot 8}{4}.$$

So in particular Tate-Shafarevich group should be trivial in this case.

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

Let ϕ be a Drinfeld module of rank 2, i.e. a homomorphism (actually an injection)

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

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, $\phi: \quad T \longrightarrow T + a_1\tau + a_2\tau^2 = \phi_T$. We can normalize ϕ as follows.

$$T \to \phi' = \lambda\phi_T\lambda^{-1} = \lambda(T + a_1\tau + a_2\tau^2)\lambda^{-1} = T + a_1\lambda^{1-q}\tau + a_2\lambda^{1-q^2}\tau^2$$

since $q = 2$ we get $T + a_1\lambda^{-1}\tau + a_2\lambda^{-3}\tau^2$, put $\lambda = a_1$ (assuming $a_1 \neq 0$) then

$$T + \tau + a_2a_1^{-3}\tau^2.$$

So Drinfeld modules are parametrized by the "j-line" $= \mathbf{P}_z^1$, as any of them can be written as $T + \tau + z^{-1}\tau^2$. In particular, the modular curve of level 1, $X(1)$, is $\mathbf{P}_z^1 = F(z)$.

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

$$\begin{aligned} aT + a^2 + z^{-1}a^4 &= 0 \\ T + a + z^{-1}a^3 &= 0 \end{aligned}$$

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.

$X_1(T^2)$ 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 $X_0(T^2) = F(a, b \cdot \phi_{1+T}(b))$.

$$\begin{tikzcd}
 & & X_1(T^3) \arrow[dl, "4"'] \arrow[d, "4"] \\
F(a,\ b \cdot \phi_{1+T} b,\ C) \arrow[d, dash] & X_0(T^3) \arrow[d, "2"'] & X_1(T^2) \arrow[dl, "2"'] \arrow[d, "4"] \\
F(a,\ b \cdot \phi_{1+T} b) \arrow[d, dash] & X_0(T^2) \arrow[d, "2"'] & X_1(T) \arrow[dl, equal] \\
F(a) \arrow[d, dash] & X_0(T) \arrow[d, "3"'] & \\
F(z) & X(1) &
\end{tikzcd}$$

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

$$a^3 Tb + a^3 b^2 + (a + T)b^4 = a^4 \tag{7}$$

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

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

Plug this into (7)

$$a^3 Tb + a^3 b^2 + (a + T)(B^2 + a^2 b^2) = a^4$$
$$a^2 T(ab + b^2) + (a + T)B^2 = a^4$$

$$a^2 TB + (a + T)B^2 = a^4 \tag{8}$$

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

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.

$$Tc + c^2 + z^{-1} c^4 = b \tag{9}$$

$(A/T^3)^\times = < 1, 1+T, 1+T^2, 1+T+T^2 >$, 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 (9) 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.

8 Heegner points from Drinfeld modular curves

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 (End(ϕ)=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 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.

Take

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

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 $E(K)$. It turns out to be the double of the generator of the infinite part (rank(E)=1).

9 Weil uniformization

The analogue of Shimura-Taniyama conjecture for function fields was known for a long time, see [1], [4]:

Theorem 9.1 (Drinfeld, Deligne, Zarhin,...) *Each elliptic curve E/F, F is a function field, with multiplicative reduction at ∞ is a quotient of a suitable Drinfeld modular curve $X_0(\mathbf{n})$.*

We still will be assuming that $A = \mathbf{F}_2[T]$ and $F = \mathbf{F}_2(T)$, although most of the statements are true for a general function field.

Let C be the completion of the algebraic closure of F_∞ and let $\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(F_\infty)$ be the Drinfeld upper half plane. The set of C points of $X_0(\mathbf{n}) - \{cusps\}$ is just $\Omega/\Gamma_0(\mathbf{n})$.

Our curve $E: \quad Y^2 + TXY = X^3 + T^2X$ was split multiplicative at ∞, so $E(C) \cong C^\times/q_E^{\mathbf{Z}}$ for some $q_E \in C^\times, \quad |q_E|_\infty < 1$. The above theorem implies the existence of a certain automorphic form φ, called *newform*, of level T^3 and corresponding to E so that, for example, $L(E,s) = L(\varphi,s)$. This newform can be computed as a harmonic function on the Bruhat-Tits tree associated to $PGL_2(F_\infty)$. Consider the composition

$$G: \quad \Omega \longrightarrow \Omega/\Gamma_0(\mathbf{n}) \hookrightarrow X_0(\mathbf{n})(C) \longrightarrow E(C) = C^\times/q_E^{\mathbf{Z}}$$

Gekeler and Reversat have given explicit analytic formulas (using theta functions) for q_E and the map G in terms of the newform φ.

This formula can be used to compute the Heegner point on E without computing the equation for $X_0(\mathbf{n})$! We proceed to describe the formula.

10 Harmonic cochains

Let $\Omega = \mathbf{P}^1(C) - \mathbf{P}^1(F_\infty)$ viewed as a rigid analytic space. Let $\Omega \longrightarrow \widetilde{\Omega}$ be the associated analytic reduction. Then $\widetilde{\Omega}$ is a scheme over k_∞ (the residue field of the place at infinity), locally of finite type. Each irreducible component M of $\widetilde{\Omega}$ is isomorphic to $\mathbf{P}^1_{k_\infty}$ and meets exactly $q_\infty + 1$ other components M'. The intersections are ordinary double points which are rational over k_∞. For example, when $F = \mathbf{F}_2(T)$, $\widetilde{\Omega}$ looks like

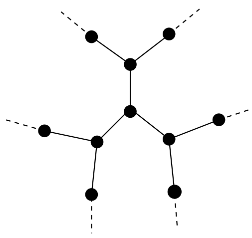

Figure 4: $\widetilde{\Omega}$

$\widetilde{\Omega}$ is canonically isomorphic to the Bruhat-Tits tree $\mathcal{T}$ of $PGL_2(F_\infty)$. Let $X(\mathcal{T})$ and $Y(\mathcal{T})$ be the vertices and edges of $\mathcal{T}$.

Definition 10.1 *A harmonic cochain (= "currency") on $\mathcal{T}$ is a map*

$$\varphi : \quad Y(\mathcal{T}) \longrightarrow \textit{abelian group (usually } \mathbf{C}\textit{)}$$

that satisfies

$$\varphi(e) + \varphi(\overline{e}) = 0 \qquad (e \in Y(\mathcal{T}))$$

and

$$\sum_{e \in Y(\mathcal{T}),\quad terminus(e)=v} \varphi(e) = 0 \qquad (v \in X(\mathcal{T}))$$

Denote $\Gamma := \Gamma_0(\mathbf{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) \quad | \quad \mathbf{n}|c \right\}$ (for most of the statements below Γ can be any arithmetic subgroup of $GL_2(A)$).

Γ acts on Ω via $z \longrightarrow (az+b)/(cz+d)$.

Theorem 10.2 (Drinfeld) $Y_0(\mathbf{n}) := \Gamma \setminus \Omega$ *is a smooth irreducible affine algebraic curve over C*

Let $X_0(\mathbf{n}) = \overline{Y_0(\mathbf{n})}$; $X_0(\mathbf{n})$ is not geometrically irreducible in general, it will have $\mathrm{Pic}(A)$ irreducible components, this corresponds to the fact that $X_0(\mathbf{n})$ as an algebraic curve is defined over the Hilbert class field H of K, but for $A = \mathbf{F}_2[T]$ it is irreducible.

There is an analytic reduction

$$\Gamma \setminus \Omega \longrightarrow \Gamma \setminus \mathcal{T}.$$

Now $\Gamma \setminus \mathcal{T} = (\Gamma \setminus \mathcal{T})^\circ \cup (\bigcup h_i)$, where $(\Gamma \setminus \mathcal{T})^\circ$ is a finite graph and h_i are finitely many half-lines (these correspond to the cusps), moreover

$$\#\mathrm{cusp}(\Gamma) := \Gamma \setminus \mathbf{P}^1(F).$$

Let $H_!(\mathcal{T}, \mathbf{Z})^\Gamma$ be the harmonic cochains on $\mathcal{T}$ invariant under Γ, i.e. $\varphi(\gamma e) = \varphi(e) \quad (\gamma \in \Gamma, \quad e \in Y(\mathcal{T}))$, and which have compact support modulo Γ. We shall consider $H_!(\mathcal{T}, \mathbf{Z})^\Gamma$ as a space of functions on the quotient graph $\Gamma \setminus \mathcal{T}$.

Theorem 10.3 *$H_!(\mathcal{T}, \mathbf{Z})^\Gamma$ is a free abelian group of rank g, where*

$$g = \dim_{\mathbf{Q}}(\Gamma^{ab} \otimes \mathbf{Q}) = \textit{genus of } X_0(\mathbf{n})$$

Γ/torsion can be canonically identified with the fundamental group of $\Gamma \setminus \mathcal{T}$ (see J.-P. Serre, *Trees*, I, Thm. 13, Cor. 1), and

$$\overline{\Gamma} := \Gamma^{ab}/\mathrm{torsion}\Gamma^{ab} \cong (\Gamma/\mathrm{torsion})^{ab} \cong H_1(\Gamma \setminus \mathcal{T}, \mathbf{Z})$$

But there is a natural map

$$H_1(\Gamma \setminus \mathcal{T}, \mathbf{Z}) \longrightarrow H_!(\mathcal{T}, \mathbf{Z})^\Gamma$$

which is injective and becomes bijective after tensoring with $\mathbf{Q}$. Hence we have a map

$$j: \quad \overline{\Gamma} \longrightarrow H_!(\mathcal{T}, \mathbf{Z})^\Gamma$$

For later calculations the following will be useful:

Theorem 10.4 *[4] When $A = \mathbf{F}_q[T]$*

$$j: \quad \overline{\Gamma} \longrightarrow H_!(\mathcal{T}, \mathbf{Z})^\Gamma$$

is an isomorphism.

Example Now we compute the quotient of the Bruhat-Tits tree by $\Gamma_0(T^3) \subset GL_2(\mathbf{F}_2[T])$, and the newform on $X_0(T^3)$ as a harmonic cochain on $\Gamma \setminus \mathcal{T}$.

Gekeler [3] has a formula for the genus of $X_0(\mathbf{n})$ but we don't really need this as we know from explicit computations that $g(X_0(T^3)) = 1$. So $\Gamma \setminus \mathcal{T}$ has one loop (and it's clear from the action of $\Gamma_0(T^3)$ on $\mathcal{T}$ that the loop has 4 edges).

$GL_2(\mathbf{F}_2[T])$ acts transitively on $\mathbf{P}^1(F)$ and the stabilizer of $(0:1)$ is

$$G_0 := \left\{ \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \quad | \quad c \in \mathbf{F}_2[T] \right\}$$

Similarly, the stabilizer of $(0:1)$ in $\Gamma_0(T^3)$ is $\Gamma_0' := \left\{ \begin{pmatrix} 1 & 0 \\ T^3c & 1 \end{pmatrix} \quad | \quad c \in \mathbf{F}_2[T] \right\}$, so

$$\sharp\mathrm{cusps}(X_0(T^3)) = (GL_2(\mathbf{F}_2[T]) \ : \ \Gamma_0(T^3))/(G_0 \ : \ \Gamma_0') = 24/6 = 4$$

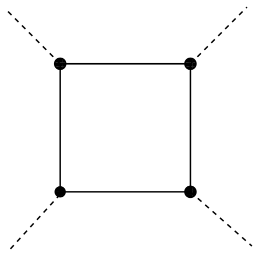

Figure 5: $\Gamma_0(T^3) \setminus \mathcal{T}$

Now it is clear that essentially there is only one harmonic cochain with compact support on $\Gamma \setminus \mathcal{T}$; 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 $\Gamma \setminus \mathcal{T}$ and the harmonic cochain we can compute the Petersson inner product on $H_!(\mathcal{T}, \mathbf{Q})^\Gamma$ which enters Gross-Zagier formula.

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

$$(\varphi, \varphi) = \sum_{e \in Y(\Gamma \setminus \mathcal{T})} \varphi(e) \cdot \varphi(e) \mu(e) = 4.$$

There are different reasonable normalizations for the measure involved in PIP though.

11 Theta functions

Let ω, and η be fixed elements of Ω, and put

$$\theta(\omega, \eta, z) = \prod_{\gamma \in \widetilde{\Gamma}} \frac{z - \gamma\omega}{z - \gamma\eta}$$

where $\widetilde{\Gamma} = \Gamma / \Gamma \cap$ center of GL_2. Since we are considering $GL_2(\mathbf{F}_2[T])$ the center is trivial, so we will be omitting tilde.

Theorem 11.1 *Let* $\alpha \in \Gamma$

(i) *The product for* $\theta(\omega, \eta, z)$ *converges locally uniformly on* Ω. *If* $\Gamma\omega \neq \Gamma\eta$, $\theta(\omega, \eta, z)$ *has a zero (pole) of order* $\sharp\Gamma\omega$ ($\sharp\Gamma\eta$) *at* ω, η, *respectively, and no other zeros or poles. If* $\Gamma\omega = \Gamma\eta$, $\theta(\omega, \eta, z)$ *has neither zeros nor poles on* Ω.

(ii) *There exists a constant* $c(\omega, \eta, \alpha) \in C^*$ *such that*

$$\theta(\omega, \eta, \alpha z) = c(\omega, \eta, \alpha) \cdot \theta(\omega, \eta, z)$$

independently of z.

(iii) $c(\omega, \eta, \alpha)$ *depends only on the class of* α *in* $\overline{\Gamma} := \Gamma^{ab}/torsion\Gamma^{ab}$.

(iv) *The function* $\theta(\omega, \eta, \alpha z)$ *is holomorphic and non-zero at the cusps of* Γ.

(v) *The holomorphic function*

$$u_\alpha(z) = \theta(\omega, \alpha\omega, z)$$

is independent of the choice of $\omega \in \Omega$. *It depends only on the class of* α *in* $\overline{\Gamma}$.

(vi) *For* $\alpha, \beta \in \Gamma$ *we have* $u_{\alpha\beta} = u_\alpha \cdot u_\beta$

(vii)

$$c(\omega, \eta, \alpha) = u_\alpha(\eta)/u_\alpha(\omega)$$

In particular, $c(\omega, \eta, \alpha)$ *is holomorphic in* ω *and* η.

(viii) *Let*

$$c_\alpha(\cdot) = c(\omega, \alpha\omega, \cdot) : \quad \Gamma \longrightarrow C^*$$

be the multiplier of u_α. *Then* $(\alpha, \beta) \longrightarrow c_\alpha(\beta)$ *defines a symmetric bilinear map from* $\overline{\Gamma} \times \overline{\Gamma}$ *to* C^*.

Proof: See [4]

Let $\varphi \in H_!(\mathcal{T}, \mathbf{Q})^\Gamma$ be a newform, which is an eigenform for the Hecke algebra with integral eigenvalues, and let φ be primitive, i.e. normalized so that $\varphi \in j(\overline{\Gamma})$ but φ is not in $n \cdot j(\overline{\Gamma})$ for $n > 1$ (recall $j : \quad \overline{\Gamma} \cong H_!(\mathcal{T}, \mathbf{Z})^\Gamma$). Let u_φ be the theta function associated to a representative of φ in Γ (label the representative also by φ).

Theorem 11.2 (Gekeler-Reversat) *Chose $\omega_0 \in \Omega$. The function $u_\varphi(z)/u_\varphi(\omega_0)$ on Ω descends to a non-constant map*

$$\begin{aligned} X_0(\mathbf{n}) &\longrightarrow E_\varphi(C) = C^*/q_E^{\mathbf{Z}} \\ z &\longrightarrow u_\varphi(z)/u_\varphi(\omega_0) \end{aligned} \tag{10}$$

where q_E is the Tate period of E.

Remark Gekeler and Reversat actually prove that $\Lambda = \{c_\varphi(\alpha) \quad | \quad \alpha \in \Gamma\} = \mu_d \times t^{\mathbf{Z}}$, where μ_d is the d^{th} root of unity $d \mid q_\infty - 1$, and $t = c_\varphi(\beta)$ for some $\beta \in \Gamma$, $t \in F_\infty^*$ with $|t|_\infty < 1$, i.e. the period also can be computed in terms of theta functions. Also note that the choice of ω_0 in (10) is arbitrary.

12 Computing the Heegner points

$E: \quad Y^2 + TXY = X^3 + T^2X$, $j(E) = T^4$.

Since we know $j(E) = T^4$, to compute Tate period just invert

$$f(q) = 1/j(q) = q - 744q^2 + 356652q^3 - \cdots$$

i.e. find $g(q) = q + \cdots \in \mathbf{Z}[[q]]$ s.t. $g(f(q)) = q$. Then $q_E = g(\frac{1}{j(E)})$. As the first few coefficients in $g(q)$ are even we may assume, to some precision, that $q_E \asymp \frac{1}{T^4}$ (we don't really need theta functions for this).

$H_!(\mathcal{T}, \mathbf{Z})^\Gamma = \mathbf{Z}\varphi$, $\overline{\Gamma} \cong H_!(\mathcal{T}, \mathbf{Z})^\Gamma$. To apply Gekeler-Reversat formula we need to find a representative of the generator of the cyclic group $\overline{\Gamma} := \Gamma_0(T^3)^{ab}/\text{torsion}\Gamma_0(T^3)^{ab}$ in $\Gamma_0(T^3)$.

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

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

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 φ 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

$$u_\varphi(U) \mod q_E^{\mathbf{Z}}$$

where $U^2 + U = T$.

To be able to approximate the infinite product

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

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 $ad - cb = 1$, $\deg(a) \leq \max\ (\deg(b), \deg(c), \deg(d)) \implies |a| \leq \max\ (|b|, |c|, |d|) \implies |b| \cdot \max\ (|c|, |d|) \geq \max\ (|a|, |b|, |c|, |d|)$, 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 $u_\varphi(U)$ 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 $\Gamma_0(\mathbf{n})$ 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

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

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

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

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

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

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. Gekeler, *Drinfeld modular curves*, LNM **1231** (1986)

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

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

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

[7] J. Silverman, *Advanced topics in the arithmetics of elliptic curves*, GTM **151**

[8] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, LNM **476** (1975)

[9] J. Tate, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Seminaire Bourbaki (1966)