EXPLICIT CALCULATIONS WITH ELLIPTIC CURVES OVER FUNCTION FIELDS

DOUGLAS ULMER

The goal of this project is to make many of the objects showing up in the Gross-Zagier computations more concrete, by working out an example in detail.

1. A pair of interesting curves

1.1. **The curves.** Let $F = \mathbb{F}_2(T)$ and consider the elliptic curve E over F with affine equation

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

and its quadratic twist E' with affine equation

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

(The quadratic extension is $K = F(U)$ where $U^2 + U = T$.) The project is to compute "everything" about these elliptic curves.

1.2. **Elementary invariants.** Start by computing the j-invariant, discriminants, reduction types, and conductors of E and E'. The key reference is [Tate75].

1.3. **Invariants entering into BSD.** Next, you can compute the Hasse-Weil L-functions of E and E'. (It helps to know that for curves like these, the degree of the L-function as a polynomial in q^{-s} is the degree of the conductor minus 4.) Once you have the L-function you know the expected ranks of $E(F)$ and $E'(F)$ and a computer search, or some judicious guessing, will turn up generators. You can then compute heights and the regulator. Finally, the BSD formula gives a prediction for the order of Ш which can be proved to be correct. (You can just assume this point if time is lacking.)

For the statement of BSD as well as a clean treatment of the "fudge factors" and periods, I recommend [Tate66]. The article of Gross in the Storrs volume [Storrs] shows how to define the canonical height in terms of intersection numbers. If you decide you need to do 2-descents, [Ulmer] might be useful.

Date: February 13, 2000.

1.4. **Heegner points algebraically.** In the first part you will have discovered that E has relatively small conductor (call it $\mathfrak{n}\infty$), split multiplicative reduction at $T=\infty$, and that K/F satisfies the hypotheses needed to obtain a Heegner point on E/K. In this part, which I hope will be the meat of the project, you will try to write down this Heegner point explicitly. The main problem is to find equations for the Drinfeld modular curve of level $\Gamma_0(\mathfrak{n})$. (Hints: First convince yourself that the modular curve of level (1) is $\mathbb{P}^1$, i.e., the j-line. Then write down the "universal" rank 2 Drinfeld module over $F(j)$, i.e., one whose j-invariant is j, and think about what a level $\Gamma_0(\mathfrak{n})$ structure amounts to. It may be useful to think about $\Gamma_0(\mathfrak{n})$ as a quotient of $\Gamma_1(\mathfrak{n})$.)

Once you have $X_0(\mathfrak{n})$ you can write down a minimal isogeny $X_0(\mathfrak{n})\to E$. (It will turn out to be of degree 1, i.e., an isomorphism.) Finally, it's reasonably easy to find rank 2 Drinfeld modules with appropriate level structure and complex multiplication. Using them, we get a point in $E(K)$. What's the relationship between this point and the generators of $E(F)$ and $E'(F)$ you found above, and between the height of the point and $L'_K(E,1)$?

As references for Drinfeld modular curves, I suggest [DH] and some of the survey articles in [Ohio] or [AB]. For Heegner points, try Section of I.3 of [GZ] or [G]. I can also provide much more elaborate hints.

1.5. **Heegner points analytically.** We know that there is a newform f of level $\mathfrak{n}\infty$ and harmonic at ∞ corresponding to E (so that, e.g., $L(E,s)=L(f,s)$). You can compute this newform explicitly, as a harmonic function on the Bruhat-Tits tree associated to $\mathrm{GL}_2(F_\infty)$. (Finding all the newforms of a given level amounts to an elaborate exercise in group theory. You can then match the newforms to isogeny classes of elliptic curves by looking at Hecke eigenvalues and counting points. In our case, there is only one newform, so the last issue does not arise.)

Now let C be the completion of the algebraic closure of F_∞ and let $\Omega=\mathbb{P}^1(C)\setminus\mathbb{P}^1(F_\infty)$ be the Drinfeld upper half plane. The set of C points of $X_0(\mathfrak{n})\setminus\{\text{cusps}\}$ is just $\Omega/\Gamma_0(\mathfrak{n})$. Also, since E is split multiplicative at ∞, $E(C)=C^\times/q_E^{\mathbb{Z}}$ for some $q_E\in C^\times$. Consider the composition

$$G:\Omega\twoheadrightarrow\Omega/\Gamma_0(\mathfrak{n})\hookrightarrow X_0(\mathfrak{n})(C)\to E(C)=C^\times/q_E^{\mathbb{Z}}.$$

Gekeler and Reversat have given explicit analytic formulas for q_E and the map G in terms of the newform f. I call them analytic because they are in terms of infinite products (indexed by the group $\Gamma_0(\mathfrak{n})$) converging in C. The last part of the project is to compute q_E and the Heegner point on E to some degree of T^{-1}-adic accuracy. Crude estimates for the convergence of the products suggest that this will require some machine computation.

References for this part are [Weil], [Gek], and [GR].

Due to the need for machine computation (and the heaviness of the preceding part!) I don't expect that this part will actually get worked on at the Winter School.

2. Variants

2.1. **Another pair of curves over F.** All of the above applies equally well to the curves

$$\begin{aligned} E :& Y^2 + TXY + TY = X^3 \\ E' :& Y^2 + TXY + TY = X^3 + T^3(T+1)^2X^2 + T^3(T+1)^2 \end{aligned}$$

Here the twisting field is $K = F(U)$ where $U^2 + U = T(T+1)^2$.

2.2. **Characteristic 3.** If characteristic 2 makes you queasy, you can consider the curve

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

over $\mathbb{F}_3(T)$ and its twists by $K = \mathbb{F}_3(T,U)$ where $U^2 = T + 1$ or $U^2 = 1 - T^2$. But be warned that 3^6 is much bigger than 2^6.

2.3. **Constant curves.** Curves with $j(E)$ in the field of constants don't fit into the Drinfeld modular picture (at least naively), and so don't have Heegner points, but they do present some interesting phenomena. To see some of them, compute "everything" for the curve

$$Y^2 = X^3 - X$$

over $F = \mathbb{F}_q(X)[Y]/(Y^2 - X^3 + X)$. Here things depend in an interesting way on q, which is assumed to be odd.

2.4. **Isotrivial curves.** Similarly for

$$Y^2 = X^3 - T$$

over $\mathbb{F}_q(T)$ (q prime to 6) or

$$Y^2 = X^3 - TX + 1$$

over $\mathbb{F}_q(T)$ where q is a power of 3. See the last section of [Weil] for some interesting automorphic aspects of these curves.

References

[AB] Gekeler, E.-U. et al., Eds: "Drinfeld Modules, Modular Schemes, and Applications" (Proceedings of a workshop at Alden-Biesen, Belgium 1996) World Scientific, Singapore, 1997

[DH] Deligne, P. and Husemöller, D.: *Survey of Drinfeld modules.* Contemporary Math. **67** (1987), 25–91

[Gek] Gekeler, E.-U.: *Automorphe Formen über $F_q(T)$ mit kleinem Führer.* Abh. Math. Sem. Univ. Hamburg **55** (1985), 111–146

[GR] Gekeler, E.-U. and Reversat, M.: *Jacobians of Drinfeld modular curves.* J. Reine Angew. Math **476** (1996), 27–93

[GZ] Gross, B. and Zagier, D.: *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), 225–320

[G] Gross, B.: *Heegner points on $X_0(N)$.* In: "Modular Forms" (ed. R. A. Rankin) pp. 87–106, Ellis Horwood, Chichester, 1984

[Ohio] Goss, D. et al., Eds: "The Arithmetic of Function Fields" (Proceedings of a conference at Columbus, OH 1991) de Gruyter, Berlin, 1992

[Storrs] Cornell, G. and Silverman, J., Eds.: "Arithmetic Geometry" (Proceedings of a conference at Storrs, CT 1985), Springer, New York, 1986

[Tate66] Tate, J.: *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog.* Séminaire Bourbaki 1965/66, Exposé 306

[Tate75] Tate, J.: *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In "Modular Forms of One Variable IV" (Lecture Notes in Math. 476) (1975), 33–52

[Ulmer] Ulmer, D.: *p-descent in characteristic p.* Duke Math. J. **62** (1991), 237–265

[Weil] Weil, A.: "Dirichlet series and automorphic forms" (Lecture Notes in Math. 189) Springer, Berlin, 1971