18.783 Elliptic Curves — **Spring 2013**

Problem Set #7 — **Due: 04/09/2013**

Description

These problems are related to the material covered in Lectures 14-15. As usual, the first person to spot each non-trivial typo/error will receive one point of extra credit.

Instructions: Solve both Problems 1 and 2, and then complete Problem 3, which is a survey. **Late problem sets will lose one point for each hour they are late**.

Problem 1. The Weil conjectures (50 points)

The *zeta function* of a smooth projective curve $C/\mathbb{F}_q$ (or more generally, a projective variety) is the exponential generating function

$$Z(C/\mathbb{F}_q;T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})T^n}{n}\right).$$

The exponential of a formal power series $F \in \mathbb{Q}[[t]]$ with constant term zero is defined by

$$\exp(F) = \sum_{k=0}^{\infty} \frac{F^k}{k!},$$

and the inverse operation is the formal logarithm[1]

$$\log(F) = \sum_{k=1}^{\infty}(-1)^{n+1}\frac{(F-1)^n}{n}.$$

The integers $\#C(\mathbb{F}_{q^n})$ can be recovered from $Z(C/\mathbb{F}_q;T)$ via

$$\#C(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(C/\mathbb{F}_q;T)\Big|_{T=0}.$$

The definition of the zeta function may seem awkward at first glance, but it has many remarkable properties. Most notably, although it is defined as a power series, it is actually a rational function.

Theorem 1 (Weil)**.** *Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g.*

1. *(Rationality) $Z(C/\mathbb{F}_q;T) = \frac{P(T)}{(1-T)(1-qT)}$ for some polynomial $P \in \mathbb{Z}(T)$ of degree $2g$.*
2. *(Functional Equation) $Z(C/\mathbb{F}_q;1/(qT)) = q^{1-g}T^{2-2g}Z(C/\mathbb{F}_q;T)$*
3. *(Riemann Hypothesis) The roots $\alpha_1,\ldots\alpha_{2g} \in \mathbb{C}$ of $P(T)$ satisfy $|\alpha_i| = 1/\sqrt{q}$.*

[1] These definitions agree with the usual Taylor series expansions; note that $\log(1-F) = -\sum_{k=1}^{\infty}\frac{F^n}{n}$.

This theorem was conjectured by Emil Artin and proved by Weil in 1949. Weil also proposed generalizations to projective varieties that include this theorem as a special case; these became known as the *Weil conjectures*. Many mathematicians contributed to the proof of the Weil conjectures, including Bernard Dwork, Michael Artin, Alexander Grothendieck, and Pierre Deligne, who completed the proof in the 1970's.[2] In this problem you will prove the Weil conjectures in the case that C is an elliptic curve E, and derive several useful facts along the way.

Most of the facts we need hold for any endomorphism of an elliptic curve E, in fact for any element of the endomorphism algebra $\mathrm{End}^0(E)$, so we will prove them in this generality and then apply them to the Frobenius endomorphism of an elliptic curve over a finite field. So let ϕ be an arbitrary element of $\mathrm{End}^0(E)$, and let $\alpha, \beta \in \mathbb{C}$ be the roots of its characteristic polynomial $x^2 - \mathrm{tr}(\phi)x + \deg(\phi)$.

1. Show that ϕ can be written uniquely as $\phi = \phi_r + \phi_i$, with $\phi_r \in \mathbb{Q}$, $\phi_i \in \mathrm{End}^0(E)$ and $\phi_i^2 = -\deg(\phi_i)$. Define $\mathrm{re}(\phi) = \phi_r \in \mathbb{R}$ and $\mathrm{im}(\phi) = \sqrt{\deg(\phi_i)} \in \mathbb{R}$, and let $\mathbb{Q}(\phi)$ denote the $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(E)$ generated by ϕ. Prove that there is a unique field embedding $\iota\colon \mathbb{Q}(\phi) \hookrightarrow \mathbb{C}$ that maps ϕ to $\mathrm{re}(\phi) + \mathrm{im}(\phi)i$, and that for all $\lambda \in \mathbb{Q}(\phi)$ we have $\iota(\hat{\lambda}) = \overline{\iota(\lambda)}$, where the bar denotes complex conjugation in $\mathbb{C}$.

2. Use part 1 to prove that $|\alpha| = |\beta| = \sqrt{\deg \phi}$ and therefore $|\mathrm{tr}(\phi)| \le 2\sqrt{\deg \phi}$.

3. By applying part 2 to the Frobenius endomorphism π of $E/\mathbb{F}_q$ and recalling that $1-\pi$ is separable, give a very short proof of Hasse's theorem: $|q + 1 - \#E(\mathbb{F}_q)| \le 2\sqrt{q}$.

4. Prove that for any positive integer n we have $\mathrm{tr}(\phi^n) = \alpha^n + \beta^n$ and therefore

$$\deg(1 - \phi^n) = \deg(\phi)^n + 1 - \alpha^n - \beta^n.$$

Deduce that if $\phi = \pi$ is the Frobenius endomorphism of $E/\mathbb{F}_q$, then

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

As a quick digression, part 4 implies that for $E/\mathbb{F}_q$ we can easily compute $\#E(\mathbb{F}_{q^n})$ once we know $\#E(\mathbb{F}_q)$. A useful method for doing this is the following recurrence.

5. Let $a_0 = 2$ and $a_n = q^n + 1 - \#E(\mathbb{F}_{q^n})$. Prove that $a_{n+2} = a_1 a_{n+1} - q a_n$ for all $n \ge 0$. Conclude that the zeta function $Z(E/\mathbb{F}_q; T)$ is completely determined by $\#E(\mathbb{F}_q)$.

You are now ready to prove the Weil conjectures for elliptic curves.

6. Prove that

$$\exp\left(\sum_{n=1}^{\infty} \frac{\deg(1-\phi^n)}{n} T^n\right) = \frac{1 - \mathrm{tr}(\phi)T + \deg(\phi)T^2}{(1-T)(1-\deg(\phi)T)}.$$

By applying this in the case that $\phi = \pi$ is the Frobenius endomorphism of $E/\mathbb{F}_q$, prove that the rationality statement in Theorem 1 holds with $P(T) = 1 - \mathrm{tr}(\pi)T + qT^2$, in the case that C is the elliptic curve E.

7. Prove that the functional equation and Riemann hypothesis in Theorem 1 both hold when C is an elliptic curve.

[2] Deligne was recently awarded the $1,000,000 Abel prize for this work.

Problem 2. An elliptic curve with complex multiplication (50 points)

Let $E/\mathbb{Q}$ be the elliptic curve defined by

$$y^2 = x^3 - 35x - 98.$$

We wish to consider the endomorphism $\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$, where

$$\begin{aligned}
u(x) &= 2x^2 + (7 - \sqrt{-7})x + (-7 - 21\sqrt{-7}),\\
v(x) &= (-3 + \sqrt{-7})x + (-7 + 5\sqrt{-7}),\\
s(x) &= 2x^2 + (14 - 2\sqrt{-7})x + (28 + 14\sqrt{-7}),\\
t(x) &= (5 + \sqrt{-7})x^2 + (42 + 2\sqrt{-7})x + (77 - 7\sqrt{-7}).
\end{aligned}$$

The following block of sage code represents $\phi = (\frac{u}{v}, \frac{s}{t})$ as a pair of rational functions in x, with the factor y in the second coordinate implicit. It then verifies that ϕ is an endomorphism of E by checking that its coordinate functions satisfy the curve equation $y^2 = f(x) = x^3 - 35x - 98$:

```
R.<t>=PolynomialRing(Rationals())
N.<d>=NumberField(t^2+7)
F.<x>=PolynomialRing(N)
u=2*x^2 + (-d + 7)*x -(7+21*d)
v=(-3+d)*x +(-7+5*d)
s=2*x^2 + (-2*d + 14)*x + (14*d + 28)
t=(5+d)*x^2 + (42+2*d)*x + (77-7*d)
phi = (u/v,s/t)
f=x^3-35*x-98
assert phi[1]^2*f == f.subs(phi[0])
```

Note: on the LHS of the `assert` we also squared the implicit y and replaced y^2 by $f(x)$.

1. Determine the characteristic polynomial of ϕ by computing (hint: its degree is evident, you just need to determine its trace $\phi + \hat{\phi}$; remember that addition in the endomorphism ring corresponds to the group operation on the elliptic curve).

2. Determine $\mathrm{End}(E)$. Be sure to justify your answer.

3. Let p be a prime of good reduction for E. Prove that the reduction of E at p is supersingular if the Legendre symbol $\left(\frac{-7}{p}\right)$ is -1 and ordinary otherwise.

4. Let p be the least prime greater than the last two digits of your student ID where E has supersingular reduction. Prove that the endomorphism algebra of $E \bmod p$ is a quaternion algebra $\mathbb{Q}(\alpha, \beta)$ with $\alpha^2, \beta^2 < 0$ and $\alpha\beta = -\beta\alpha$. Give α^2 and β^2 explicitly, and express α and β in terms of ϕ and the Frobenius endomorphism π.

5. Prove that every prime p where E has ordinary reduction satisfies the norm equation

$$4p = t^2 + 7v^2,$$

   where $t = \mathrm{tr}\,\pi$ is the trace of Frobenius and v is a positive integer.

6. Find a pair of primes $p, q > 2^{512}$ for which the reduction of E modulo p has exactly $4q$ rational points. Be sure to format your answer so that the primes p and q both fit on the page (line wrapping is fine).

Problem 3. Survey

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
4/2	Endomorphism algebras				
4/4	Ordinary and supersingular curves				

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

18.783 Elliptic Curves
Spring 2013