Description

These problems are related to the material covered in Lectures 13-14. As usual, the first person to spot each non-trivial typo/error will receive one point of extra credit.

Instructions: Solve **one** of Problems 1 and 2, and then complete the survey Problem 3.

Problem 1. The Weil conjectures (100 points)

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

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

The exponential of a formal power series $F \in \mathbb{Q}[[t]]$ with zero constant term is given 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 $Z(C; T)$ via

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

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

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

(i) *(rationality)* $Z_C(T) = \frac{P(T)}{(1-T)(1-qT)}$ *for some $P \in \mathbb{Z}(T)$ of degree $2g$.*

(ii) *(functional equation)* $Z_C(\frac{1}{qT}) = q^{1-g}T^{2-2g}Z_C(T)$

(iii) *(Riemann hypothesis) The roots $\alpha_1, \ldots \alpha_{2g} \in \mathbb{C}$ of $P(T)$ satisfy $|\alpha_i| = 1/\sqrt{q}$.*

This theorem was conjectured by Emil Artin in 1924 and proved by Weil in 1949. Weil also proposed generalizations of the three parts of the theorem to smooth projective varieties of arbitrary dimension; these became known as the *Weil conjectures*. Many mathematicians contributed to the proof of the Weil conjectures, including Bernard

---

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

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 for elliptic curves and derive several useful facts along the way.

The proof relies on various properties of the Frobenius endomorphism, most of which actually hold for any endomorphism of any elliptic curve E/k, in fact, for any element of the endomorphism algebra $\text{End}^0(E) := \text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, 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 $\text{End}^0(E)$, and let $\alpha, \beta \in \mathbb{C}$ be the roots of its characteristic polynomial $x^2 - \text{tr}(\phi)x + \deg(\phi)$.

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

(b) Use part (a) to prove that $|\alpha| = |\beta| = \sqrt{\deg \phi}$ and therefore $|\text{tr}(\phi)| \leq 2\sqrt{\deg \phi}$.

(c) By applying part (b) 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: $|q+1-\#E(\mathbb{F}_q)| \leq 2\sqrt{q}$.

(d) Prove that for any positive integer n we have $\text{tr}(\phi^n) = \alpha^n + \beta^n$ 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 (d) 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.

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

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

(f) Prove that

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

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

(g) Prove that the functional equation (ii) and Riemann hypothesis (iii) in Theorem 1 hold when C is an elliptic curve.

---

[2]Deligne was awarded both the Fields medal (1978) and the Abel prize (2013) for this work.

You may be wondering why $Z_E(T)$ is called a zeta function, and how it relates to the *Riemann zeta function*

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The sum on the RHS converges for complex s with real part greater than 1, and it extends to a unique analytic function $\zeta(s)$ that is defined on all of $\mathbb{C}$ except for a simple pole at $s = 1$. The *normalized Riemann zeta function* $\xi(s) := \pi^{s/2}\Gamma(s/2)\zeta(s)$ satisfies the *functional equation*[3]

$$\xi(s) = \xi(1 - s),$$

and the *Riemann hypothesis* states that the zeros of $\xi(s)$ all lie on the *critical line* $\{s \in \mathbb{C} : \mathrm{Re}(s) = 1/2\}$.

For an elliptic curve $E/\mathbb{F}_q$ we define

$$\zeta_E(s) := Z_E(q^{-s}).$$

(h) Prove that $\zeta_E(s) = \zeta_E(1 - s)$.

(i) Prove that every zero of $\zeta_E(s)$ lies on the critical line $\{s \in \mathbb{C} : \mathrm{Re}(s) = 1/2\}$.

You may recall that the Riemann zeta function has an *Euler product*

$$\zeta(s) = \prod_{p} \left(1 - p^{-s}\right)^{-1},$$

where p ranges over all primes. The function $\zeta_E(s)$ also has an Euler product that can be written as a product over points $P \in E(\overline{\mathbb{F}}_q)$, but in this product we don't want to distinguish points P and Q that are *Galois conjugate*, meaning that $Q = \sigma(P)$ for some automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. We thus define the *closed point*

$$\overline{P} := \{\sigma(P) : \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\}.$$

The set $\overline{P}$ is the orbit of $P \in E(\overline{\mathbb{F}}_q)$ under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. It is a finite set because P lies in some finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. Indeed, if $\mathbb{F}_{q^n}/\mathbb{F}_q$ is the minimal such extension then $\#\overline{P} = n$ (because $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order n). We now define $N(\overline{P})$ to be the cardinality of this minimal extension; it is well-defined because $N(\overline{Q}) = N(\overline{P})$ whenever $\overline{Q} = \overline{P}$ (so it is an invariant of $\overline{P}$, not just P).

(j) Prove that

$$\zeta_E(s) = \prod_{\overline{P}} \left(1 - N(\overline{P})^{-s}\right)^{-1}$$

where $\overline{P}$ ranges over all closed points of $E(\overline{\mathbb{F}}_q)$.

---

[3]Here $\pi = 3.1415\ldots$ and $\Gamma(t) := \int_0^{\infty} x^{t-1}e^{-x}dx$.

Problem 2. An elliptic curve with complex multiplication (100 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

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

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 $f(x)$.

(a) Determine the characteristic polynomial of ϕ.

(b) 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.

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

(d) 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.

(e) Prove that every prime p where E has ordinary reduction satisfies the norm equation

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

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

(f) Find a pair of primes $p, q > 2^{512}$ for which the reduction E_p 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).

(g) Describe a probabilistic algorithm that, given a sufficiently large integer n, outputs two integers p and q that have passed 100 Miller Rabin tests with $p \in [2^n, 2^{n+1}]$ such that if p is prime, then $\#E_p(\mathbb{F}_p) = q$ (we can be morally certain that both p and q are in prime, but the algorithm is not required to guarantee this).

Under the heuristic model that each integer m is prime with probability $1/\log m$, bound the expected running time of your algorithm and compare it an alternative approach that generates random curves and counts points using Schoof's algorithm (your algorithm should be significantly faster; in fact, it should be faster than any method known for proving the primality of a general n-bit integer — this is why we do not want to require the algorithm to guarantee that p and q are prime).

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
3/19	Endomorphism algebras				
3/31	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 2015