Math 581b, Fall 2010, Homework 8

William Stein

Due: November 24, 2010

Do the following 3 problems, and turn them in by Wednesday, November 24, 2010. As usual, you can find the latex of this file at `http://wstein.org/edu/2010/581b/hw/`. You may use mathematics software however you want in this problem set.

This will be the last homework assignment of this course. All the future work for credit that you'll do in this class after this assignment will focus entirely on your final project.

1. Watch the excellent 45-minute documentary *The Proof*, if you haven't already: `http://video.google.com/videoplay?docid=8269328330690408516`.

2. (a) Define integers a_n by the infinity product

   $$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum a_n q^n,$$

   Compute (somehow) the numbers a_p for $p = 2, 3, 5, 7, 13, 17, 19$. (Hint: In Sage, typing `R.<q> = QQ[[]]` makes the q the generator of a power series ring over $\mathbf{Q}$, which can be handy.)

   (b) Let E be the elliptic curve $y(y+1) = x^2(x-1)$. Define primes numbers a_p by

   $$a_p = p + 1 - \#E(\mathbf{F}_p).$$

   (The curve E has bad reduction at $p = 11$, and we define $a_{11} = 1$.) Compute the numbers a_p for $p = 2, 3, 5, 7, 13, 17, 19$. You should get the same numbers as in the previous part above. (Hint: In Sage, typing `E.ap(p)` computes a_p, if E is an elliptic curve, created using the `EllipticCurve` command.)

3. In this problem you will explore the basis of Schoof's algorithm for point counting, which makes elliptic curve cryptopgraphy possible. Let E be the elliptic curve $y^2 = x^3 + 3x + 7$ over the finite field $\mathbf{F}_p$, where p is the "massive prime" 10009. (Hint: You can create E in Sage by typing `E = EllipticCurve(GF(10009),[3,7])`.)

   (a) Compute $E[3](\overline{\mathbf{F}}_p)$ explicitly. Hint: We have $E[3](\overline{\mathbf{F}}_p) = E[3](\mathbf{F}_{p^2})$, so you can do

```
sage: F = E.change_ring(F(10009^2,’a’))
sage: F(0).division_points(3)
```

(b) Compute the matrix of Frob_p acting on the 2-dimensional $\mathbf{F}_3$ vector space $E[3]$, with respect to some basis of your choosing. There is no “nice way” to do this in Sage, so don’t worry if your code is just ugly.

(c) It must be the case that $\mathrm{Trace}(\mathrm{Frob}_p) = a_p$, so if you take the trace of the above matrix you should get $p + 1 - \#E(\mathbf{F}_p)$ modulo 3.

```
sage: 10009  + 1 - E.cardinality()
70
```