Appendix: Counting points on $E(F_q)$

References: http://www.math.ucla.edu.~gschaeff/crypto/Schoof.pdf

Audrey Terras Fourier **Analysis on Finite Groups and Applications** (Finite Fields pg 63)

Use the Frobenius map $\varphi: Fq \rightarrow F_q : a \rightarrow a^p$

Where $q = p^r$ and p is prime. Let F_5 and F_{25} be finite fields mod 5

Elements of $F_{25}(\alpha)^*$, $\alpha^2+\alpha+1=0$ where $\alpha^i = a_0+a_1\alpha$, with α_j in F_5 .

TABLE I Calculation of $(x+y*\alpha)^2$ and $(x+y*\alpha)^3-(x+y*\alpha)-1$

$X+Y*\alpha$	$(x+y*\alpha)^2$ mod(5)	$(x+y*\alpha)^3-(x+y*\alpha)-1$ mod(5)
0	0	4
$0+\alpha$	$4+4\alpha$	4α
$0+2\alpha$	$1+\alpha$	$2+3\alpha$
$0+3\alpha$	$1+\alpha$	$1+2\alpha$
$0+4\alpha$	$4+4\alpha$	$3+\alpha$
1	1	4
$1+\alpha$	α	$2+4\alpha$
$1+2\alpha$	2	$3+\alpha$
$1+3\alpha$	$2+2\alpha$	$4+\alpha$
$1+4\alpha$	2α	2
2	4	0
$2+\alpha$	$3+3\alpha$	0
$2+2\alpha$	4α	$4+3\alpha$
$2+3\alpha$	3α	$3+4\alpha$
$2+4\alpha$	3	$3+3\alpha$
3	4	3
$3+\alpha$	3	2α
$3+2\alpha$	3α	3α
$3+3\alpha$	4α	$4+2\alpha$
$3+4\alpha$	$3+3\alpha$	$3+4\alpha$
4	1	4
$=4+\alpha$	2α	3
$4+2\alpha$	$2+4\alpha$	0
$4+3\alpha$	2	$3+3\alpha$
$4+4\alpha$	4α	$4+\alpha$

In the above table $F_{25} \sim F_5(\alpha)/(\alpha^2+\alpha+1)$ where $\alpha^2+\alpha+1=0$ and is irreducible over F_5.

The above table is used to find the finite solutions to $y^2 = x^3 - x - 1$ since $\alpha^2 = -(\alpha+1) = 4\alpha + 4$, and $\alpha^3 = 1$.

Matching row 3 with row 2 there are a total of 26 solutions plus the point at infinity or $\#E(F_{25}) = 27$.

Then $\#E(F_{25}) = q + 1 - a_q(25)$

So $a_q(25) = -1$

Every element in $F_{25} \sim F_5(\alpha)$ has the form $a_0 + a_1\alpha$ where a_0 and a_1 are in F_5.

Based on the above reference the Frobenius map can be used to calculate the value of $a_p(5)$.

Summarizing the calculations below I show that

$E(F_{25})[3] = \{P \in \mathcal{E}(F_{25}) : 3P = \mathbf{O}\} \sim Z/3Z \times Z/3Z$

Let P =(4,2) and Q = $(3,3+\alpha)$ be two points which are on the elliptic curve. It can be shown with the group law on Elliptic Curves (See Ash, **Fearless Symmetry**, pg 107 that 3P = P+P+P = **O** and

3Q = **O**. (Also known as 3-torsion).

The subgroup of $E(F_{25})$ generated by P and Q is " isomorphic to Z/3Z X Z/3Z.

As indicated in Chalkboard #12 we can calculate the Frobenius character such that:

$\chi(Frob_p) = a_p$

By finding the trace of the matrix of the Galois representation $\varphi(Frob_q)$.

By example $\varphi(P) = P$; the point (4,2) is found in a solution to $E(F_5)$.

It can also be shown that $\varphi(Q) = -Q$ since $\varphi(3) = 3$ and

$\varphi(3+\alpha) = \varphi(\alpha) + 3 = 4\alpha + 4 + 3 = 4\alpha + 7 = 4\alpha + 2 \bmod(5) = -(3+\alpha) \bmod(5)$

The Frobenius matrix is (Note: -1 = 2 mod (3))

$$\varphi(Frobq) := \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \bmod (3)$$

And trace $\chi(Frob_p) = a_p$

= 3 (mod p) = -2 mod 5

This result agrees with the calculation for a_5 in Chalkboard #12.

A series of identities for the coefficients of the modular form are mentioned in the literature of modular form :

1. a(mn) = a(m)*a(n) whenever GCD (m,n) = 1
2. $a(p^s)*a(p) = a(p^{s+1}) + p\, a(p^{s-1})$ for a prime p and s =1 or s>1.

If s = 1 then (2) becomes: $a(p)*a(p) = a(p^2) + p*a(1)$.

If a(1) = 1 then for p = 5

a(25) = a(5)*a(5) – 5.

(-1) = -2*(-2) -5 = 4-5 = -1

The values for a(25) and a(5) calculated above agree with this modular identity.

RT