Counting point on Markov surfaces over finite fields

Cole Miller

October 24, 2017

This is a condensed account of the work of Mariscal. I have omitted most of his exposition and several results and computations that are irrelevant here, as well as changing some notation.

The setting

Let $\mathbb{F}_q$ be the finite field of q elements. We consider the *Markov*[1]*equation*

$$x^2 + y^2 + z^2 = axyz + b \tag{1}$$

for $(x, y, z) \in \mathbb{F}_q^3$, where $a, b \in \mathbb{Z}/(p)$ are parameters. Let $M^3_{a,b}(\mathbb{F}_q)$ be the set of points in $\mathbb{F}_q^3$ solving this equation. We will compute the number $|M^3_{1,b}(\mathbb{F}_q)|$ of points in $M^3_{1,b}(\mathbb{F}_q)$; we're especially interested in how $|M^3_{1,b}(\mathbb{F}_q)|$ depends on q, and it will turn out that $|M^3_{1,b}(\mathbb{F}_q)| \sim q^2$. (We aren't interested in the case of general a, although Mariscal gives it.)

[1] I prefer this spelling to Mariscal's "Markoff".

We recall that a *nonzero* element $k \in \mathbb{Z}/(n)$ is said to be a *quadratic residue* mod n if there exists $\ell \in \mathbb{Z}/(n)$ such that $\ell^2 = k$; otherwise, it is said to be a *quadratic nonresidue*. For p a prime and $a \in \mathbb{Z}/(p)$, the *Legendre symbol* is defined by[2]

$$_a\lambda_p = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \\ 0 & \text{if } a = 0 \end{cases} \tag{2}$$

[2] The Legendre symbol is usually written $\left(\frac{a}{p}\right)$, but I object to this notation so strongly that I have used my own here.

We also know that a finite field of order q exists iff $q = p^m$ for some prime p and positive integer m, and that in this case we can consider $\mathbb{F}_q$ as a $\mathbb{Z}/(p)$-vector space. Henceforth we will assume $p \neq 2$.

Computations

Calculating $|M^2_{a,b}(\mathbb{F}_q)|$

In order to compute $|M^3_{1,b}(\mathbb{F}_q)|$, we first study the "two-dimensional" analogue of the Markov equation (1), namely

$$x^2 + y^2 = axy + b, \tag{3}$$

where $(x, y) \in \mathbb{F}_q^2$. We will denote the solution set of this equation by $M^2_{a,b}(\mathbb{F}_q)$. The relevance of the lower-dimensional quantities

$|M^2_{a,b}(\mathbb{F}_q)|$ is that we have

$$|M^3_{1,b}(\mathbb{F}_q)| = \sum_{k\in\mathbb{F}_q} |M^2_{k,b-k^2}(\mathbb{F}_q)|, \tag{4}$$

since

$$x^2 + y^2 + z^2 = xyz + b \Leftrightarrow x^2 + y^2 = z(xy) + (b - z^2). \tag{5}$$

Basically, we are partitioning the three-dimensional Markov surface into two-dimensional "slices"—which turn out to just be two-dimensional Markov surfaces!

To calculate $|M^2_{a,b}(\mathbb{F}_q)|$ we specialize according to the values of a and b. In the following we will assume $q > 2$.

Suppose first that $a = \pm 2$. In this case we can manipulate (3) to obtain

$$(x \mp y)^2 = b. \tag{6}$$

Clearly this equation has no solutions (x, y) if b is a quadratic non-residue mod q. If $b = 0$ then each choice of x gives exactly one corresponding value for y such that (x, y) is a solution. Finally, if b is a quadratic residue mod q then it has two distinct square roots mod q, and in this way we get $2q$ solution pairs (x, y).

Now suppose that $a^2 - 4 \neq 0$ and $b = 0$. Clearly in this case $(0, 0) \in M^2_{a,b}(\mathbb{F}_q)$, and this is the only such point with a zero coordinate. So we may assume that $y \neq 0$. Dividing by y^2 in (**??**) and completing the square gives

$$\left(\frac{x}{y}^2 - \frac{a}{2}\right)^2 = \frac{a^2 - 4}{4} \tag{7}$$

Note that $(a^2 - 4)/4$ is a quadratic residue iff $a^2 - 4$ is. If $a^2 - 4$ is a quadratic residue, as before we have two possible values for x/y; and since we count the single case where $x = 0$ or $y = 0$ separately we get $(q - 1) + (q - 1) + 1 = 2q - 1$ solution pairs (x, y) altogether.

Next we make a linear change of variables:

$$X = x - \frac{a}{2}y \tag{8}$$

$$Y = y \tag{9}$$

With these substitutions and a small amount of algebra, (3) becomes

$$X^2 = \left(\frac{a^2 - 4}{4}\right) Y^2 + b \tag{10}$$

(Note that we have simply completed the square again.) We use this form to compute the remaining cases of $|M^2_{a,b}(\mathbb{F}_q)|$.

We continue to assume $b \neq 0$ (as the cases with $b = 0$ have already been considered). Suppose first that $(a^2 - 4)/4$, hence $a^2 - 4$, is a quadratic residue, say $k^2 = (a^2-4)/4$ with $k \neq 0$. Make another change of variables, as follows:

$$U = k(X+Y) \tag{11}$$

$$V = X - Y \tag{12}$$

Then (10) takes the form

$$UV = \frac{b}{a^2-4} \tag{13}$$

This gives $q-1$ solution pairs (U, V), in one-to-one correspondence with solution pairs (x, y) to (3). (Once again, one solution pair is unviable since neither x nor y may be 0.)

Now we tackle the last and least tractable case. Suppose that $b \neq 0$ and that $a^2 - 4$ is a quadratic nonresidue. Following Mariscal, we first note two results about the numbers of residues and nonresidues in certain subsets of $\mathbb{F}_q$. We use the notation R_q for the set of (nonzero) residues in $\mathbb{F}_q$ and N_q for the set of nonresidues.

Theorem. *Suppose $q \equiv 1 \mod 4$, and let $r \in R_q$ and $n \in N_q$. Then the cosets $r + N_q$ and $n + R_q$ each contain $\frac{q-1}{4}$ residues and $\frac{q-1}{4}$ nonresidues.*

Theorem. *Suppose $q \equiv 3 \mod 4$ and let r, n as before. Then the cosets $r + N_q$ and $n + R_q$ each contain 0 along with $\frac{q-3}{4}$ residues and $\frac{q-3}{4}$ nonresidues.*

We apply these results to the expression

$$\left(\frac{a^2-4}{4}\right) Y^2 + b \tag{14}$$

appearing in (10). There are several cases to consider (!):

- Suppose that $b \in N_q$ and $q \equiv 1 \mod 4$. Since the product of a nonresidue with a residue is a nonresidue, the term $\left(\frac{a^2-4}{4}\right) Y^2$ ranges over the set $N_q \cup \{0\}$ for $Y \in \mathbb{F}_q$. The complement of $b + N_1 \cup \{0\}$ is $b + R_q$, which contains $\frac{q-1}{4}$ residues by our first theorem; hence $b + N_q \cup \{0\}$ contains precisely the $\frac{q-1}{4}$ remaining residues. Since each element of R_q has two square roots we obtain 4 solution pairs (X, Y) for each residue value of $\left(\frac{a^2-4}{4}\right) Y^2 + b$. We also get an additional 2 solutions for $Y = 0$, giving a total of $q+1$ solutions.
- Suppose that $b \in N_q$ and $q \equiv 3 \mod 4$. The calculations go through much as previously, except that there are now fewer nonzero residues in $b + N_q \cup \{0\}$, with the compensation of two additional solutions with $X = 0$. The total remains $q+1$.

The other two cases are similar; in each case we find $q+1$ solutions.

Computing $M^3_{1,b}(\mathbb{F}_q)$

We now break the sum (4) into pieces that we can analyze according to the cases presented in the previous section. This will unfortunately involve a final bout of case-splitting.

For the first case, suppose that b and $b-4$ are residues of $\mathbb{F}_q$. We can decompose

$$|M^3_{1,b}(\mathbb{F}_q)| = 2|M^2_{2,b-4}(\mathbb{F}_q)| + 2|M^2_{\sqrt{b},0}(\mathbb{F}_q)| \tag{15}$$

$$+ \sum_{k^2 \neq 4,b} |M^2_{k,b-k^2}(\mathbb{F}_q)| \tag{16}$$

The sum (16) involves only cases of $|M^2_{a,b}(\mathbb{F}_q)|$ where $b \neq 0$ and $a^2 - 4 \neq 0$. We have

$$|M^2_{2,b-4}(\mathbb{F}_q)| = 2q \tag{17}$$

$$|M^2_{\sqrt{b},0}(\mathbb{F}_q)| = 2q - 1 \tag{18}$$

$$\sum_{k^2 \neq 4,b} |M^2_{k,b-k^2}(\mathbb{F}_q)| = \left(\frac{q-3}{2} - 2\right)(q-1) + \left(\frac{q-1}{2}\right)(q+1) \tag{19}$$

by applying the analysis from the previous section and using our theorems again. Plugging these in gives

$$|M^3_{1,b}(\mathbb{F}_q)| = q^2 + 4q + 1 \tag{20}$$

in this case.

Similar calculations apply in the other cases, with some shifting of terms and adjustments to various constants. Ultimately we find $|M^3_{1,b}(\mathbb{F}_q)| = q^2 + (3+\delta)\varepsilon q + 1$, where

$$\delta = {}_b\lambda_p \tag{21}$$

$$\varepsilon = {}_{b-4}\lambda_p \tag{22}$$