Polynomials Over Finite Fields Whose Values are Squares

T. Kyle Petersen

April 15, 2001

Abstract

This paper seeks to explain in the simplest terms possible a paper written by Umberto Zannier. Though Zannier says that his is "a simple elementary method," there are still steps in his paper that are quite subtle. The tools needed to follow his proof are in the hands of most Algebra students, though which tools to use and how to use them may not be obvious. This essay hopes to make the path from conception to conclusion as clear and easy as possible, with simple proofs and examples to show the way.

1 Introduction

Zannier's paper [Za] gives a new method for determining a lower bound for the number of solutions to congruences of the form $y^2 \equiv f(x) \pmod{p}$, where f is a polynomial (i.e. points on the curve $Y^2 = f(X)$ over the field $\mathbf{F}_p$). As he himself acknowledges, there are several other methods for estimating a lower bound for the number of solutions to such equations. Zannier's method is especially notable in that for certain cases, the estimate his method gives improves on the bounds derived from André Weil's conjectures [Ha] on the Riemann Hypothesis for curves over finite fields.

Before we mention Weil's implications, a brief rundown of other work relating to curves over finite fields is in order. We intentionally avoid the details of the Riemann Hypothesis *per se*[1], and begin with Hasse's Theorem [Si] for elliptic curves. It was Helmut Hasse's work in the 30s that was

[1]The analogue of the Riemann Hypothesis for curves over finite fields is core to the work

generalized to higher dimensional varieties in 1949 by the Weil conjectures. They remained conjectures until they were proven by Pierre Deligne [De74] [De80] in 1973. The analogue of the Riemann Hypothesis for finite fields was also proved independently by Enrico Bombieri [Bo76] in 1976. To gain some perspective on the weight of this work, note that both men are Fields' Medal winners – Bombieri in 1974, Deligne in 1978. (Bombieri called Deligne's work on the Weil conjectures "one of the crowning achievements of twentieth century mathematics." [Bo00]). The results of these great mathematicians are far-reaching and among the great accomplishments in 20th century mathematics, with applications in number theory, algebraic geometry, and discrete mathematics. That said, we turn back to the much narrower scope of our particular curve.

Hasse's result in the case of our curve $Y^2 = f(X)$ is interpreted as follows: Let $f(X) = a_0X^d + a_1X^{d-1} + \ldots + a_n \in \mathbf{F}_q$ of degree d with no repeated roots. Define $N = \#\{(x, y) \in \mathbf{F}_q^2 : y^2 = f(x)\}$. Hasse's theorem, in the case $\deg f = 3$, gives bounds of the form

$$|N - q - 1| \leq 2\sqrt{q}.$$

Weil proved the following more general statement:

$$\begin{array}{rl} |N - q| \leq (d-1)\sqrt{q} & \text{if } d \text{ is odd} \\ |N - q + 1| \leq (d-2)\sqrt{q} & \text{if } d \text{ is even and } a_0 \text{ is square in } \mathbf{F}_q \\ |N - q - 1| \leq (d-2)\sqrt{q} & \text{otherwise.} \end{array}$$

Although Weil proved certain bounds for N, the generality of his work prevents some accuracy, as we shall see. (Notice that when $d \geq 3 + \sqrt{q}$ Weil's result is trivial.) But what Zannier gains in accuracy, unfortunately, he loses in scope. He mentions that his method may be applied to more general curves, but this possibility appears less than likely. His method seems to be dependent on certain nice properties of squares, but if we had some sort of curve $f(X, Y) = 0$, these nice properties disappear. Also note that Zannier's paper does come with restrictions. First, the thrust of the paper applies only to fields of prime order. While there is a generalization of his method to fields with orders of prime power, the result is not as strong. Further, the

produced by the mathematicians mentioned here, but the details and broader implications of the famous problem fall outside the scope of this essay. See Bombieri's web article [Bo00] for more on the Riemann Hypothesis proper.

method only provides a lower bound to the number of solutions, and that bound is nontrivial only when $d < \sqrt{2q} - \frac{3}{2}$. But for $\sqrt{2q} - \frac{3}{2} > d > 3 + \sqrt{q}$, Zannier's bound is better than Weil's. So despite the somewhat narrow focus of the paper, its method is original and quite powerful for our class of curves, $Y^2 = f(X)$. Further, what makes Zannier's paper nice (apart from the result) is the accessibility it offers. Though his proof is quite clever, the tools needed to interpret it can be found in most good Algebra books. On the other hand, the tools employed by Deligne and Bombieri are (necessarily) much more sophisticated, and hence, more inaccessable.

2 Preliminary Observations

As usual, $\mathbf{F}_q$ will be used to denote the finite field of q elements, and $\mathbf{F}_q^*$ will denote the nonzero elements in a field of q elements. We assume that q is some odd prime power.

Theorem 1 *For G a finite group, and for any $a \in G$, $a^{|G|} = 1$, where $|G|$ is the order of G and 1 is the identity.*

This is an easy consequence of Lagrange's Theorem (see [He]). Since for any a in G, the order of a divides the order of G, we have $m|(a)| = |G|$ for some m. Then $a^{|G|} = a^{m|(a)|} = 1^m = 1$.

Theorem 2 *The group of nonzero elements of a field, $\mathbf{F}_q^*$, is cyclic.*

Notice that the nonzero elements of a field form an abelian group, and since the order of $\mathbf{F}_q^*$ is $q-1$, every element is a root of the polynomial $X^{q-1} - 1$, by Theorem 1. But this polynomial has at most $q-1$ roots in any field, so all the roots of the polynomial, the $(q-1)$-th roots of unity, are exactly the elements of $\mathbf{F}_q^*$. Now just notice that the set of the roots of unity is a cyclic group generated by any primitive root of unity.

Theorem 3 *For any a, b in $\mathbf{F}_q^*$, ab is square if a and b are both square or both non-square. Otherwise ab is non-square.*

Let $q = 2r + 1$. We have that $\mathbf{F}_q^*$ is a cyclic group of order $2r$. Call s its generator, so that $\mathbf{F}_q^* = \{1, s, s^2, \ldots, s^{2r-1}\}$. Let $a = s^k$ and $b = s^l$. Then $ab = s^{k+l}$. Now if a, b are both square, k, l are both even, and $k + l$ is even; hence, ab is square. If a, b are both non-square, k, l are both odd, and $k + l$ is even; hence, ab is square. If a is square, b is non-square, then k is even and l is odd. Then $k + l$ is odd, and ab is non-square.

3 Statement of Theorem and Example

Strangely, the theorem we prove says nothing (directly) of the number of solutions to our congruence. However, a corollary of the theorem will. First we need a definition:

> Let p be a prime number, and let $d(p)$ be the least positive integer d with the following property: There exists a non-square polynomial $f \in \mathbf{F}_p[X]$ of degree d, such that its values are all squares in $\mathbf{F}_p$.

Now we may state

(Zannier) Theorem 4 *For $d(p)$ even, $d^2(p) + 3d(p) \geq 2p + 2$. For $d(p)$ odd, $d^2(p) + 2d(p) \geq 2p + 1$. By completing the square, we can restate it as $d(p) \geq \sqrt{2p + \frac{17}{4}} - \frac{3}{2}$ or*

$$d(p) > \sqrt{2p} - \frac{3}{2}$$

(resp. $d(p) \geq \sqrt{2p+2} - 1$, still greater than $\sqrt{2p} - \frac{3}{2}$).

This theorem relates to the number of solutions to $y^2 = f(x)$ (with $y \neq 0$) in the following way: Let f be any polynomial of degree $d < \sqrt{2p} - \frac{3}{2}$ with at least one simple root (i.e. root of multiplicity 1) and define

$$S := \{u \in \mathbf{F}_p : \ f(u) \text{ is a nonzero square in } \mathbf{F}_p\}.$$

Define $g(X) := \prod_{u \in S}(X - u)$, then choose some non-square a in the field and consider $h(X) = g(X)^2 a f(X)$. This polynomial gives only square values, yet is non-square (by Theorem 3)[2]. So by Zannier's Theorem, $2 \deg g + d \geq d(p) > \sqrt{2p} - \frac{3}{2}$. Notice that $2 \deg g$ is exactly the number of solutions $(x, y) \in \mathbf{F}_p^2$ that we hope to find. We conclude that $\sqrt{2p} - \frac{3}{2} - d$ is a good lower bound for N, which, if d is also greater than $3 + \sqrt{p}$, improves on Weil's estimate.

[2] If $u \in S$, then $g(u) = 0 = h(u)$. If $u \notin S$, $f(u)$ is not square, but neither is a, so $af(u)$ is square and so is $h(u)$. Since a is non-square, h will be a non-square polynomial unless f looks like some $b \prod f_i^2$ for b non-square. But since we required f to have at least one simple root, this case never occurs.

As an easy example to demonstrate the method Zannier develops to prove Theorem 4, we try to prove the following, in a style similar to that of the main argument:

For $q = 2r + 1 > 3$ an odd prime power, and cubic $f \in \mathbf{F}_q[X]$, the equation $y^2 = f(x)$ has at least one solution $(x_0, y_0) \in \mathbf{F}_q^2$.

Suppose the claim is false: that there are no solutions in $\mathbf{F}_q^2$. Then for any $u \in \mathbf{F}_q$, $f(u) \neq 0$ (zero is trivially square). Then we can apply our Theorem 1 to observe that for all $u \in \mathbf{F}_q$, $f(u)^{q-1} = f(u)^{2r} = 1$. This implies that $f(u)^r = 1$ or -1. Recall from Theorem 2 that $\mathbf{F}_q^*$ is a cyclic group of order $q - 1 = 2r$. Call s the generator of $\mathbf{F}_q^* = \{1, s, s^2, \ldots, s^{2r-1}\}$. Let $f(u) = s^k$. If $f(u)^r = 1$ for some u, then $f(u)^r = s^{kr} = 1 = s^{2r}$. But then $2r|kr$, $\Rightarrow k$ is even; i.e. $f(u)$ is square. So it must be that $f(u)^r = -1$ for all $u \in \mathbf{F}_q$. Then every element of $\mathbf{F}_q$ is a root of $f(X)^r + 1$ and by the division algorithm we can write

$$f(X)^r + 1 = (X^q - X)S(X) \tag{1}$$

where $S \in \mathbf{F}_q[X]$ has degree $3r - q = r - 1$. We can now differentiate both sides of the equation to get

$$\begin{aligned} rf'(X)f(X)^{r-1} &= (X^q - X)S'(X) + S(X)(qX^{q-1} - 1) \\ &= (X^q - X)S'(X) - S(X) \end{aligned} \tag{2}$$

as $qX^{q-1} \equiv 0 (\text{mod } q)$.

Multiplying (1) by $rf'(X)$ yields:

$$rf'(X)f(X)^r + rf'(X) = rf'(X)(X^q - X)S(X).$$

Multiplying (2) by $f(X)$ yields:

$$rf'(X)f(X)^r = f(X)(X^q - X)S'(X) - f(X)S(X).$$

Subtracting these two gives:

$$\begin{aligned} rf'(X) &= rf'(X)(X^q - X)S(X) + f(X)S(X) - f(X)(X^q - X)S'(X) \\ &= (X^q - X)(rf'(X)S(X) - f(X)S'(X)) + f(X)S(X) \end{aligned}$$

or

$$rf'(X) - f(X)S(X) = (X^q - X)(rf'(X)S(X) - f(X)S'(X)). \tag{3}$$

The LHS has degree $3+r-1 = r+2$ and (X^q-X) divides it, so $r+2 = \text{degLHS} \geq q = 2r + 1$ so $r \leq 1$ and $q \leq 3$. This is a contradiction, so there must be some solution.

4 Main Arguments

We now go on to prove Theorem 4. Suppose that for $p \geq 3$, prime, $f \in \mathbf{F}_p[X]$ has degree $d \leq p-3$. Suppose further that f is non-square, but that f gives only square values in $\mathbf{F}_p$. Just as with integers, polynomials have a unique representation as the product of irreducible polynomials. So write the decomposition $f(X) = a\prod_{i=1}^{h} f_i(X)^{m_i}$ where the f_i are irreducible monic polynomials in $\mathbf{F}_p[X]$, the m_i are positive integers, and $a \in \mathbf{F}_p^*$ (i.e. nonzero). Later we'll want to say that f has a simple root. To do this we need to reduce f yet retain the properties that we are concerned with: that it is a non-square and gives only square values. A given polynomial of this type can be reduced to a more 'basic' polynomial associated with the same f_i that carries the same desired properties. (We may even be able to reduce to a polynomial of degree $d(p)$.) Given arbitrary f with its decomposition as above, we may obtain this 'basic' polynomial f^* in the following manner:

$$\begin{aligned} \text{If } m_i \text{ even, } m_i^* &= 2 \quad (\text{factor out } f_i(X)^{m_i-2}\ ) \\ \text{If } m_i \text{ odd, } m_i^* &= 1 \quad (\text{factor out } f_i(X)^{m_i-1}\ ) \end{aligned}$$

The non-square property of the polynomial is obviously retained in f^* since we are factoring out even powers. To check the property that f^* gives all square values, rewrite $f(X) = g(X)^{2n}h(X)$ where $g(X)$ is one of our monic irreducibles f_i, $h(X)$ is the unit a times the product of the remaining factors, and $2n$ is the (even) power on g we are factoring out. See that since f gives all squares and g^{2n} is square already, it must be that h gives all square values on $\mathbf{F}_p$.

So we need only concern ourselves with polynomials of degree $d = d(p)$ and whose irreducible factors have power m_i equal 1 or 2. Consider one such $f(X) = a\prod_{i=1}^{h} f_i(X)^{m_i} \in \mathbf{F}_p[X]$. Since $d \leq p-3 < p$, there are at most d distinct roots of f, so there is some $u \in \mathbf{F}_p$ such that $f(u) \neq 0$. That is, $f(u)$ is a nonzero square in $\mathbf{F}_p$. If all the $m_i = 2$, then a would be a nonzero square and $f(X)$ would be a square in $\mathbf{F}_p[X]$. So one of the $m_i = 1$, and f must have at least one simple root α, in some finite field. For example, (X^2+1) could be one of our irreducible polynomials in $\mathbf{F}_7[X]$. (X^2+1) has no root in a field of seven elements, but if we look at a field of 49 elements, there is a root, (e.g. $\mathbf{Z}[i]/7\mathbf{Z}$).

Now let $u \in \mathbf{F}_p$. Set $p = 2r+1$. Remember that f gives all squares, so either $f(u) = 0$, or using Theorem 1 again and taking $f(u) = a = b^2$ $(a, b \in$

$\mathbf{F}_p$), we have $f(u)^{p-1} = f(u)^{2r} = a^{2r} = b^{4r} \Rightarrow f(u)^r = a^r = b^{2r} = b^{p-1} = 1$. Then $f(X)(f(X)^r - 1)$ has as roots all the roots of $X^p - X$ (though it may have more in another field). Using the division algorithm, we can write

$$f(X)^{r+1} - f(X) = (X^p - X)S(X), \tag{4}$$

where $S(X) \in \mathbf{F}_p[X]$ has degree $(r+1)d - p$. Differentiating (4) gives

$$(r+1)f'(X)f(X)^r - f'(X) = (X^p - X)S'(X) + S(X)(pX^{p-1} - 1)$$

or

$$(r+1)f'(X)f(X)^r - f'(X) = (X^p - X)S'(X) - S(X), \tag{5}$$

as $pX^{p-1} = 0$. Just as with the example, multiply (4) by $(r+1)f'(X)$ and (5) by $f(X)$. Subtracting yields

$$-rf(X)f'(X) = (r+1)f'(X)(X^p - X)S(X) - f(X)(X^p - X)S'(X) + f(X)S(X)$$

or

$$f(X)S(X) = (X^p - X)(f(X)S'(X) - (r+1)f'(X)S(X)) - rf(X)f'(X). \tag{6}$$

Equation (6) is the result of the first step in an induction argument. To help the argument run smoother, Zannier creates "differential operators" Δ_m on $\mathbf{F}_p[X]$ to keep track of the induction step. He also creates S_m and R_m as placeholders for parts of the equation to keep things from getting to cluttered as the process is iterated. These will also be key in the argument of degrees that will conclude the proof. So for $\phi \in \mathbf{F}_p[X]$, define

$$\Delta_m(\phi)(X) := f(X)\phi'(X) - (r+m+1)f'(X)\phi(X),$$

and set, for $m \geq 0$,

$$\begin{aligned} S_0(X) &:= S(X) \quad & S_{m+1} &:= \Delta_m(S_m)(X) \\ R_0 &:= -rf(X)f'(X) \quad & R_{m+1} &:= \Delta_m(R_m)(X). \end{aligned}$$

Now (6) is just

$$f(X)S_0(X) = (X^p - X)S_1(X) + R_0(X). \tag{7}$$

We want to show inductively that

$$(m+1)f(X)S_m(X) = (X^p - X)S_{m+1}(X) + R_m(X). \tag{8}$$

For $m = 0$, we have (7).

Before continuing, note the following properties of Δ_m. First note how it acts on products of polynomials. For $\phi, \psi \in \mathbf{F}_p[X]$, we show $\Delta_m(\phi\psi) = \phi\Delta_m(\psi) + \phi' f\psi$.

$$\begin{aligned}\Delta_m(\phi\psi)(X) &= f(X)(\phi\psi)'(X) - (r+m+1)f'(X)(\phi\psi)(X)\\ &= f(X)(\phi(X)\psi'(X) + \psi(X)\phi'(X)) - (r+m+1)f'(X)\phi(X)\psi(X)\\ &= f(X)\psi(X)\phi'(X) + \phi(X)(f(X)\psi'(X) - (r+m+1)f'(X)\psi(X))\\ &= \phi(X)\Delta_m(\psi)(X) + f(X)\psi(X)\phi'(X)\end{aligned}$$

since $f(X)\psi'(X) - (r+m+1)f'(X)\psi(X) = \Delta_m(\psi)(X)$. It also follows immediately from the definition that $\Delta_m(\phi) - f'\phi = \Delta_{m+1}(\phi)$.

$$\Delta_m(\phi) - f'\phi = f\phi' - (r+m+1)f'\phi - f'\phi = f\phi' - (r+m+2)f'\phi = \Delta_{m+1}\phi.$$

Suppose now that the assertion is true for some $m > 0$ and apply Δ_m to both sides of (8). (This may get a little messy, but once we substitute the placeholders, it will look better.) This action yields:

$$(m+1)[f(X)\Delta_m(S_m)(X) + f'(X)f(X)S_m(X)]$$

$$= (X^p - X)\Delta_m(S_{m+1})(X) - f(X)S_{m+1}(X) + \Delta_m(R_m)(X)$$

But substituting (8) makes the left-hand side look like

$$(m+1)f(X)\Delta_m(S_m)(X) + [(X^p - X)S_{m+1}(X) + R_m(X)]f'(X)$$

or

$$(m+1)f(X)S_{m+1}(X) + f'(X)(X^p - X)S_{m+1}(X) + f'(X)R_m(X).$$

After adding $f(X)S_{m+1}(X)$ to both sides we have

$$(m+2)f(X)S_{m+1}(X) + f'(X)(X^p - X)S_{m+1}(X) + f'(X)R_m(X)$$

$$= (X^p - X)\Delta_m(S_{m+1})(X) + \Delta_m(R_m)(X)$$

or equivalently

$$(m+2)f(X)S_{m+1}(X)$$

$$= (X^p - X)[\Delta_m(S_{m+1})(X) - f'(X)S_{m+1}(X)] - f'(X)R_m(X) + \Delta_m(R_m)(X).$$

But recall that $\Delta_m\phi - f'\phi = f\phi' = \Delta_{m+1}\phi$. So more concisely now we can see that

$$(m+2)f(X)S_{m+1}(X) = (X^p - X)\Delta_{m+1}(S_{m+1})(X) + \Delta_{m+1}(R_m)(X)$$
$$= (X^p - X)S_{m+2}(X) + R_{m+1}(X), \tag{9}$$

which proves our inductive claim.

Now remember the fact that f has a simple root α. Then Zannier proves the following

CLAIM: *Let $m < r$. Then α cannot be a double root of S_m. Specifically, and more importantly, $S_m \neq 0$ for $m < r$.*

First, recall the following property of simple roots: α is a multiple root of some nonzero polynomial $f \Leftrightarrow f'(\alpha) = 0$. Also recall from equation 5 with $m = 0$:

$$(r+1)f'(X)f(X)^r - f'(X) = (X^p - X)S'(X) - S(X).$$

Since $f(\alpha) = 0$, we have $S(\alpha) - (\alpha^p - \alpha)S'(\alpha) = f'(\alpha)$. Then since α is a simple root of f (i.e. $f'(\alpha) \neq 0$), it cannot be that both $S(\alpha)$ and $S'(\alpha)$ are zero. Now assume that the claim is true for some $m < r$ and suppose that α is a double root of S_{m+1}. By definition, we have

$$S_{m+1} = \Delta_m(S_m)(X) = f(X)S'_m(X) - (r+m+1)f'(X)S_m(X).$$

Since $f(\alpha) = 0$, we have $-(r+m+1)f'(\alpha)S_m(\alpha) = 0 \Rightarrow S_m(\alpha) = 0$ because $f'(\alpha) \neq 0$ and $r + m + 1 \leq 2r < p$. Now we differentiate and obtain

$$S_{m+1}(X) = f(X)S''_m(X) + f'(X)S'_m(X) - (r+m+1)[f'(X)S'_m(X) + f''(X)S_m(X)],$$

which, when evaluated at α, gives $0 = S_{m+1}(\alpha) = -(r+m)f'(\alpha)S'_m(\alpha) \Rightarrow S'_m(\alpha) = 0$ for the same reasons as above. Then α is a double root of S_m, contrary to the assumption, and the Claim is proved.

Now that we know $S_m \neq 0$ for certain m, we finish the proof by comparing degrees as in the example. Define

$$\rho_m := \deg R_m,$$

$$\sigma_m := \deg S_m,$$

and assume the zero polynomial has degree $-\infty$. See from how we defined R_0 that $\rho_0 = d + (d-1) = 2d-1$. Also as defined, we can see that $\rho_{m+1} \leq \rho_m + d - 1$ or

$$\rho_m \leq (m+2)d - m + 1 = d + (m+1)(d-1). \tag{10}$$

We already know that $\sigma_0 = \deg S = (r+1)d - p$. Using (8) we see that

$$(X^p - X)S_{m+1}(X) = (m+1)f(X)S_m(X) - R_m(X)$$

from which we derive

$$\sigma_{m+1} \leq \max(\rho_m, d + \sigma_m) - p.$$

Now using(10) we have

$$\sigma_{m+1} \leq \max((m+1)(d-1), \sigma_m) + d - p.$$

Now suppose that

$$\sigma_m \geq (m+1)(d-1) \tag{11}$$

is true for $m = 0, ..., M-1$ but not for $m = M$. Notice that $\sigma_0 = (r+1)d - p = (r+1)d - (2r+1) = (d-2)r + (d-1) \geq d-1$, so that $M \geq 1$. And now from above, $\sigma_{m+1} \leq \sigma_m + d - p$ for $m \leq M-1$ and

$$\sigma_m \leq \sigma_0 + m(d-p) = rd - (m+1)(p-d) \tag{12}$$

for $m \leq M$. Considering both (11) and (12), with $m \leq M-1$, $(m+1)(d-1) \leq \sigma_m \leq rd - (m+1)(p-d) \Rightarrow (m+1)(p-1) = (m+1)2r \leq rd$. Then we have

$$M \leq d/2. \tag{13}$$

Notice also that since $d \leq p-3 = 2r-2$, $M \leq \frac{d}{2} \leq r-1$, which means by our Claim, that $S_{M+1} \neq 0$. (If d odd, then $M \leq \frac{d-1}{2}$, $d \leq p-4$, and still $M \leq r-1$.) Then by our formula we know $0 \leq \sigma_{M+1} \leq (M+1)(d-1) + d - p$ which when we consider (13) means

$$2p \leq d^2 + 3d - 2 \text{ if } d \text{ even}$$

$$2p \leq d^2 + 2d - 1 \text{ if } d \text{ odd.}$$

5 Additional Results

1. In the general case of $\mathbf{F}_q$, where $q = p^m$, the proof still goes through, but the result is weaker. We can just replace p with q until the Claim. There we need to be worried about multiples of p, so instead of requiring $m \leq r$ (where $q = 2r+1$), it must be only for $m \leq r_0$ where $p = 2r_0+1$. The final statement is that $d \geq \min(r_0, \sqrt{2q} - \frac{3}{2})$. Now the lower estimate for the number of solutions to $y^2 = f(x)$ is worse than before, namely $N \geq \min(r_0, \sqrt{2q} - \frac{3}{2}) - d$.

2. Very notably, the same method employed in the proof can be used to find directly a lower bound for the number of nonzero solutions to $y^2 = f(x)$. This bound is actually better than the one found as a corollary of Theorem 4. We only need to begin with a specific polynomial determined by f. To form this polynomial, define $S := \{u \in \mathbf{F}_p : f(u)$ is not a square in $\mathbf{F}_p\}$ and let $g(X) := \prod_{u \in S}(X - u)$. Now rather than (4) from above we have

$$g(X)f(X)(f(X)^r - 1) = (X^p - X)S(X).$$

Every step of the proof still makes perfect sense; we only need to modify our differential operator to

$$\Delta_m(\phi) := g(X)f(X)\phi'(X) - [(r+m+1)g(X)f'(X) + (m+1)g'(X)f(X)]\phi(X),$$

which arises from the differentiation now of the product. Working through, we can conclude that

$$2 \deg g \geq \frac{4(p-1)}{d+4} - 2(d-1).$$

If we choose any non-square a, then this conclusion applied to $af(X)$ gives us $2 \deg g$ as the number of solutions we want.

References

[Bo00] Bombieri, E. Problems of the Millenium: The Riemann Hypothesis. *Millenium Prize Problems*, www.claymath.org, (2000).

[Bo76] Bombieri, E. Hilbert's 8th Problem: An Analogue. *AMS Proc. of Symposia in Pure Math.* 28 (1976), p.269-274.

[De74] Deligne, P. La Conjecture de Weil I. *Publications Math. IHES* 43, (1974), p.273-308.

[De80] Deligne, P. La Conjecture de Weil II. *Publications Math. IHES* 52, (1980), p.137-252.

[Ha] Hartshorne, R. *Algebraic Geometry*. Springer-Verlag, New York (1977), p.449-458.

[He] Herstein, I.N. *Topics in Algebra* 2^{nd} ed. Wiley & Sons, New York, (1975).

[Si] Silverman, J.H. *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York (1986).

[Za] Zannier, U. Polynomials Modulo p Whose Values Are Squares (Elementary Improvements on Some Consequences of Weil's Bounds). *L'Enseignement Mathématique.* t. 44 (1998), p.95-102.