§1. Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **44 (1998)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

L'Enseignement Mathématique, t. 44 (1998), p. 95–102

POLYNOMIALS MODULO p WHOSE VALUES ARE SQUARES (ELEMENTARY IMPROVEMENTS ON SOME CONSEQUENCES OF WEIL'S BOUNDS)

by Umberto ZANNIER

ABSTRACT. We introduce a simple elementary method to prove lower bounds for the number of solutions of congruences of the type $y^2 \equiv f(x) \pmod{p}$. When the degree d of f does not exceed $\sqrt{2p}-(3/2)$, the estimates are nontrivial. In particular, for $\sqrt{2p} - (3/2) > d > 3 + \sqrt{p}$ we improve on what follows from the Riemann Hypothesis for a hyperelliptic function field. We illustrate the method by proving a lower bound for the minimal degree of a non-square polynomial all of whose values on $\mathbf{F}_p$ are squares in $\mathbf{F}_p$.

§ 1. INTRODUCTION

The present note arose with the author's attempt to describe to undergraduate students a proof 'as quick as possible' of the fact that congruences like $y^2 \equiv f(x) \pmod{p}$ usually have some solution [1]).

Concerning such congruences, many methods and results are offered by the literature. We may mention e.g. a method based on Gaussian sums ([Mo, p.39]) which works in special cases. Also, we have of course Hasse's Theorem in case f has degree 3 (see [Sil] for a recent exposition) and its far reaching generalization provided by Weil's Riemann Hypothesis for curves over finite fields.

We recall briefly that Weil's results imply in particular an estimate for the number of $\mathbf{F}_q$-rational points of an absolutely irreducible nonsingular projective curve defined over $\mathbf{F}_q$. To apply the theorem to our hyperelliptic affine curve $Y^2 = f(X)$, where $f(X) = a_0X^d + \cdots + a_d \in \mathbf{F}_q[X]$ has

[1]) This is of course useful in testing whether a given hyperelliptic affine curve over $\mathbf{Q}$ has points locally everywhere, i.e. over all $\mathbf{Q}_p$.

degree d, one must take into account a nonsingular projective model. The conclusion is as follows. Suppose that f has no repeated roots and define $N := \#\{(x,y) \in \mathbf{F}_q^2 \ : \ y^2 = f(x)\}$. Then

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

Weil's original proof [We] was quite sophisticated. Subsequently, elementary proofs were found independently by Bombieri and Schmidt, both arguments stemming from a method by Stepanov, who was in fact able to treat the equations we are considering here (see the survey [Bo] and the book [Sch]). Also, we point out the work by Stark [St] on hyperelliptic curves and the work by Stöhr and Voloch [SV] (which contains the full Weil bound); in both papers certain improvements on Weil's results are obtained in some cases.

The mentioned proofs, while more elementary than Weil's, are however quite delicate. Here we present a very simple method which seems new. Though it does not imply (1), it leads with minimal effort to the existence of solutions as soon as the characteristic exceeds some function of the degree. (See e.g. the beginning of §2 for a short example.)

Actually, in some cases we may go beyond (1). Note that (1) becomes trivial when $d \geq 3+\sqrt{q}$. Our method, in case q is a prime, gives something nontrivial provided $d < \sqrt{2q}-(3/2)$. (Stark, too, sometimes improves on (1), but he requires $d \leq 3+\sqrt{q}$.) The present proofs are similar to those of Stark, in that they use the iteration of certain differential operators. However we do not need to construct auxiliary functions (as in Stark's arguments) and our recursion formulae are extremely simple. It is quite possible that the method falls into the much more general and conceptual setting developed by Stöhr and Voloch (who remark that their ideas may lead to improvements on Weil in many special cases); however we have not attempted to carry out such a reconstruction.

To illustrate the method, we focus on the following simply stated problem and postpone to §3 some detail for a more general application. Let p be a prime number and define $d(p)$ as the least positive integer d with the following property:

($\star$) *There exists a polynomial $f \in \mathbf{F}_p[X]$ of degree d, not the square of a polynomial in $\mathbf{F}_p[X]$, such that its values on $\mathbf{F}_p$ are all squares in $\mathbf{F}_p$.*

What sort of function is $d(p)$?

Define $m(p)$ as the minimal positive integer m such that $p^m > m2^p$. We have $m(p) \sim p\log 2/\log p$. In §3.3, we shall show in a simple way that $d(p) \leq 2m(p)$ (perhaps an essentially optimal bound). Proving good lower bounds for $d(p)$ is more difficult. With the help of (1) it is easy to show that $d(p) > \sqrt{p}$. This is essentially the best that we can extract from (1). In fact, we have already remarked that (1) does not provide any information for $d > 3 + \sqrt{p}$. Here we give a short elementary proof of the following

THEOREM. *We have* $d^2(p) + 3d(p) \geq 2p + 2$, *hence* $d(p) \geq \sqrt{2p} - \frac{3}{2}$.

An immediate corollary is that the number of solutions in $\mathbf{F}_p^2$ of $y^2 = f(x)$ with $y \neq 0$, is at least $\sqrt{2p} - \frac{3}{2} - d$, provided $f \in \mathbf{F}_p[X]$ has degree d and at least one simple root. In fact, let

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

and put $g(X) := \prod_{u\in S}(X - u)$. Then observe that if a is a quadratic non-residue mod p, the polynomial $g(X)^2 af(X)$ assumes only square values on $\mathbf{F}_p$, without being a square. The theorem implies $2\deg g + d \geq \sqrt{2p} - \frac{3}{2}$. On the other hand, $2\deg g$ is precisely the number of solutions we are considering. We shall outline in §3.2 how to improve on this bound.

§2. MAIN ARGUMENTS

We start with a simple example to outline the origin of the method. We give a self-contained nine-line proof of the following claim: *Let* $q = 2r + 1 > 3$ *be an odd prime power and let* $f \in \mathbf{F}_q[X]$ *be a cubic polynomial. Then the equation* $y^2 = f(x)$ *has at least one solution* $(x_0, y_0) \in \mathbf{F}_q^2$.

(Mordell [Mo, p. 41] had to invoke fairly complicated arguments even to deal with the special case $f(X) = X^3 + k$.)

Assume the assertion false. Then $f(u)^r = -1$ for all $u \in \mathbf{F}_q$. Hence every element of $\mathbf{F}_q$ is a root of $f(X)^r + 1$ and so, identically,

$$f(X)^r + 1 = (X^q - X)S(X), \tag{2}$$

where $S \in \mathbf{F}_q[X]$ has degree $3r - q = r - 1$. Differentiating the equation we get

$$rf'(X)f(X)^{r-1} = (X^q - X)S'(X) - S(X). \tag{3}$$

Multiply (2) by $rf'(X)$, (3) by $f(X)$ and subtract to obtain