

**Zeitschrift:** L'Enseignement Mathématique  
**Band:** 44 (1998)  
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

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

**Kapitel:** §3. Remarks  
**Autor:** Zannier, Umberto  
**DOI:** <https://doi.org/10.5169/seals-63899>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 15.10.2024

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

$$(11) \quad \rho_m \leq d + (m + 1)(d - 1).$$

Also, from (5), (10) and (11) we get (recalling our definition of  $\deg 0$ ),

$$(12) \quad \begin{cases} \sigma_0 = (r + 1)d - p \\ \sigma_{m+1} \leq \max(\sigma_m + d, \rho_m) - p \leq \max(\sigma_m, (m + 1)(d - 1)) + d - p. \end{cases}$$

Observe that we have  $\sigma_0 = (r + 1)d - p = (r + 1)d - (2r + 1) = (d - 2)r + (d - 1) \geq d - 1$ . Suppose that the inequality

$$(13) \quad \sigma_m \geq (m + 1)(d - 1)$$

is true for  $m = 0, \dots, M - 1$ , but not for  $m = M$  (possibly  $M = \infty$ ). Then  $M \geq 1$ . Moreover, by (12) we have  $\sigma_{m+1} \leq \sigma_m + d - p$  for  $m \leq M - 1$ , whence

$$(14) \quad \sigma_m \leq \sigma_0 + m(d - p) = rd - (m + 1)(p - d), \quad \text{for } m \leq M.$$

Applying (13) and (14) with any  $m \leq M - 1$ , we get  $rd - (m + 1)(p - d) \geq (m + 1)(d - 1)$ , i.e.  $2r(m + 1) \leq rd$ . Therefore we have

$$(15) \quad M \leq \frac{d}{2}.$$

Finally, apply (12) for  $m = M$  and observe that  $M \leq d/2 \leq r - 1$ , hence  $S_{M+1} \neq 0$  by the Claim. We obtain  $0 \leq \sigma_{M+1} \leq (M + 1)(d - 1) + d - p$ , whence, comparing with (15),

$$2p \leq \begin{cases} d^2 + 3d - 2 & \text{if } d \text{ is even} \\ d^2 + 2d - 1 & \text{if } d \text{ is odd.} \end{cases}$$

This proves the theorem and more.  $\square$

### §3. REMARKS

(1) The method gives some information also in the case of a general finite field  $\mathbf{F}_q$ . The same arguments as above work everywhere, on replacing  $p$  by  $q$ , except that in the Claim we must now suppose that  $m \leq r_0$ , where  $p = 2r_0 + 1$ . The final conclusion will be that  $d \geq \min(r_0, \sqrt{2q} - (3/2))$ . This is still sufficient to prove that equations  $y^2 = f(x)$  in  $\mathbf{F}_q$  have some solution, provided  $p$  is sufficiently large compared to  $\deg f$ .

(2) The same method of proof produces a lower bound for the number  $N'$  of solutions of  $y^2 = f(x)$  such that  $y \neq 0$ . This bound is better than the one which has been stated above, as a corollary of the theorem itself. To

derive this bound we define  $S := \{u \in \mathbf{F}_p : f(u) \text{ is not a square in } \mathbf{F}_p\}$  and put  $g(X) := \prod_{u \in S} (X - u)$ . Then we observe that

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

This equation generalizes (5) above. At this point we follow completely the above proof of the theorem. The differential operators will now be defined by

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

The conclusion will be that

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

Apply this result with  $af(X)$  in place of  $f(X)$ , where  $a$  is a quadratic nonresidue in  $\mathbf{F}_p$ . Then observe that the left side is just  $N'$ .

(3) As announced in §1, we give a simple proof of the upper bound  $d(p) \leq 2m(p)$  (defined in the introduction). Define  $N_c$  as the number of monic polynomials in  $\mathbf{F}_p[X]$  which are irreducible and have degree  $c$ . By counting elements in the field  $\mathbf{F}_{p^c}$  we easily find the following formula (which goes back to Gauss), i.e.

$$\sum_{r|c} rN_r = p^c,$$

the sum running over positive divisors of  $c$ . For  $c \geq 3$  this easily implies

$$\sum_{2 \leq d \leq c} N_d \geq \frac{p^c}{c}.$$

Let  $g(X) \in \mathbf{F}_p[X]$  be monic, irreducible of degree  $d \geq 2$  and consider the vector whose entries are the Legendre symbols  $\left(\frac{g(u)}{p}\right)$ , for  $u \in \mathbf{F}_p$ . Since each entry lies in  $\{\pm 1\}$ , the number of possibilities for the vector is  $\leq 2^p$ . If we let  $g$  run through all such polynomials, with  $2 \leq d \leq c$ , the number of possibilities for  $g$  will be  $\geq p^c/c$ . For  $c = m(p)$ , this quantity exceeds  $2^p$  by definition. Hence there will be distinct choices  $g_1(X), g_2(X)$  for  $g(X)$ , giving rise to the same vector. This means that the polynomial  $f(X) := g_1(X)g_2(X)$  assumes nonzero square values on the whole of  $\mathbf{F}_p$ . Moreover, since  $g_1, g_2$  are distinct, monic and irreducible,  $f(X)$  has no square factor of positive degree. Therefore we have  $d(p) \leq \deg f \leq 2m(p)$ , as stated.