

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de 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)
Autor: Zannier, Umberto
Kapitel: §2. Main arguments
DOI: <https://doi.org/10.5169/seals-63899>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 06.08.2025

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

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,

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

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

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

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

$$(4) \quad rf'(X) = (X^q - X)(rf'(X)S(X) - f(X)S'(X)) + f(X)S(X).$$

Observe now that $rf'(X) - f(X)S(X)$ has degree $3 + \deg S = r + 2$ and is divisible by $X^q - X$, in view of (4). Hence $r + 2 \geq q = 2r + 1$, i.e. $r \leq 1$ and $q \leq 3$. \square

We now prove the theorem. Suppose that $f \in \mathbb{F}_p[X]$ ($p > 3$) has degree $d \leq p - 3$, is not a square in $\mathbb{F}_p[X]$ but assumes on \mathbb{F}_p only values which are squares in \mathbb{F}_p . Write $f(X) = a \prod_{i=1}^h f_i(X)^{m_i}$, where $a \in \mathbb{F}_p^*$, the $f_i \in \mathbb{F}_p[X]$ are distinct monic irreducible polynomials and the m_i are positive integers. Factoring out suitable even powers of the f_i , we may assume²⁾ that $1 \leq m_i \leq 2$. Since $d < p$, there exists $u \in \mathbb{F}_p$ with $f(u) \neq 0$, so $f(u)$ is a nonzero square in \mathbb{F}_p . If all the m_i were even, then a would be a nonzero square in \mathbb{F}_p and f would be a square in $\mathbb{F}_p[X]$, contrary to assumptions. Therefore at least one of the m_i is equal to 1, proving that f has at least a simple root α (in some finite field).

Let now $u \in \mathbb{F}_p$. Then, writing $p = 2r + 1$, either $f(u) = 0$ or $f(u)^r = 1$. Therefore $f(X)(f(X)^r - 1)$ is divisible by $X^p - X$. We write

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

where $S \in \mathbb{F}_p[X]$ has degree $(r + 1)d - p$. Differentiate (5) to obtain

$$(6) \quad (r + 1)f'(X)f^r(X) - f'(X) = (X^p - X)S'(X) - S(X).$$

Similarly to the above example, multiply (5) by $(r + 1)f'(X)$, (6) by $f(X)$ and subtract. The result is

$$(7) \quad f(X)S(X) = (X^p - X)(f(X)S'(X) - (r + 1)f'(X)S(X)) - rf(X)f'(X).$$

This equation is the first step in a recursion that we are going to construct. Define the differential operators Δ_m on $\mathbb{F}_p[X]$ by setting, for $\phi \in \mathbb{F}_p[X]$,

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

and put, for $m \geq 0$,

$$(8) \quad \begin{cases} S_0(X) := S(X), & S_{m+1}(X) := \Delta_m(S_m)(X), \\ R_0(X) := -rf(X)f'(X), & R_{m+1}(X) := \Delta_{m+1}(R_m)(X). \end{cases}$$

Then (7) reads

$$(9) \quad f(X)S_0(X) = (X^p - X)S_1(X) + R_0(X).$$

²⁾ Note that when m_i is even we cannot factor out $f_i(X)^{m_i}$ without danger of destroying the properties of $f(X)$. In fact we could have a priori $f(u) = f_i(u) = 0$ for some $u \in \mathbb{F}_p$ while $(f/f_i^{m_i})(u)$ could be a non-square in \mathbb{F}_p . It is however safe to factor out $f_i^{m_i-2}$.

We shall prove by induction that for all $m \geq 0$ we have

$$(10) \quad (m+1)f(X)S_m(X) = (X^p - X)S_{m+1}(X) + R_m(X).$$

For $m = 0$ this is just (9). Assume (10) true and apply to both sides the operator Δ_m . Note that $\Delta_m(\phi\psi) = \phi\Delta_m(\psi) + \phi'f\psi$. We obtain

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

Now use (10) to substitute for $(m+1)fS_m$ in the second term of the left side. We get

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

whence

$$(m+2)fS_{m+1} = (X^p - X)(\Delta_m(S_{m+1}) - f'S_{m+1}) + \Delta_m(R_m) - f'R_m.$$

Now, to conclude the inductive argument we have only to note that $\Delta_m(\phi) - f'\phi$ equals just $\Delta_{m+1}(\phi)$.

Recall that f has a simple root α . We continue by proving the following

CLAIM. *Let $m \leq r$. Then α cannot be a double root of S_m . In particular, $S_m(X) \neq 0$ for $m \leq r$.*

For $m = 0$ this follows at once from (5). Suppose the claim true for a certain m and assume by contradiction that α is a double root of $S_{m+1}(X) = f(X)S_m'(X) - (r+m+1)f'(X)S_m(X)$, where $m+1 \leq r$. Then, first of all we would have $(r+m+1)f'(\alpha)S_m(\alpha) = 0$. This implies that $S_m(\alpha) = 0$, since $f'(\alpha) \neq 0$ and since $r+m+1 \leq 2r = p-1$. Next, we compute

$$\begin{aligned} S_{m+1}'(X) &= f'(X)S_m'(X) + f(X)S_m''(X) \\ &\quad - (r+m+1)f''(X)S_m(X) - (r+m+1)f'(X)S_m'(X). \end{aligned}$$

Since $f(\alpha) = S_m(\alpha) = S_{m+1}'(\alpha) = 0$, we obtain that $-(r+m)f'(\alpha)S_m'(\alpha) = 0$. As before, this implies that $S_m'(\alpha) = 0$. Hence α would be a double root of $S_m(X)$, a contradiction to the inductive assumption.

As in the example, we shall conclude by comparison of degrees. Define

$$\rho_m := \deg R_m, \quad \sigma_m := \deg S_m,$$

where we may agree that the zero polynomial has degree $-\infty$. We have $\rho_0 = 2d-1$ and we derive directly from the recursion formulae (8) that $\rho_{m+1} \leq \rho_m + d-1$, whence

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

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