

Objektyp: **Abstract**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **27.04.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 solution¹).

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 $\mathbf{Q}_p$.