Vol. 71, No. 3 DUKE MATHEMATICAL JOURNAL © September 1993

SUMS OF SQUARES OVER FUNCTION FIELDS

KATHY D. MERRILL AND LYNNE H. WALLING

Given a polynomial α with coefficients in a finite field $\mathbb{F}$, how many ways can we represent α as a sum of k squares? The answer to this question is all too often "infinity". Thus instead, we ask: What is the value of the "restricted representation number"

$$r(\alpha, m) = \# \left\{(\beta_1, \ldots, \beta_k) : \sum_j \beta_j^2 = \alpha \text{ and } \deg \beta_j < m \right\}?$$

Jacobi and Hardy used the theory of elliptic functions and powers of the classical theta series to solve the analogous problem over $\mathbb{Z}$ for $k \leqslant 8$. Later, Hardy and Ramanujan introduced techniques that led to asymptotic formulae for the classical representation numbers with $k > 4$ (see [3]).

In this paper we too will use powers of a theta function to study the restricted representation numbers $r(\alpha, m)$ where α lies in the polynomial ring $\mathbb{F}[T]$ (T an indeterminate); the theta function $\theta(z)$ we use was recently presented in [5]. After some preliminary remarks, we show that $\theta(z)$ transforms under the "full modular group" Γ (see Theorem 2.4). Then using rather elementary techniques, we derive a formula for $r(\alpha, m)$. This formula involves Kloosterman sums when $\deg \alpha \geqslant 4$, but we are able to compute: (1) the average value of $r(\alpha, m)$; (2) the order of magnitude of $r(\alpha, m)$ as $m \to \infty$ or $\deg \alpha \to \infty$; and (3) an asymptotic formula for $r(\alpha, m)$ as k, the number of squares, approaches ∞ (see Theorems 3.11, 3.14, and 3.15 resp.).

For a full account of the history of this problem over $\mathbb{Z}$, the reader is referred to [2]. To read about the modular group over a function field, the reader is referred to [9]and [5].

The authors thank Jeff Hoffstein and Jeff Stopple for many helpful conversations.

1. Preliminaries. Let $\mathbb{A} = \mathbb{F}[T]$ where $\mathbb{F}$ is a finite field and T is an indeterminate. For the sake of clarity, we treat only the case where $\mathbb{F}$ has p elements, p an odd prime. We denote the field of fractions of $\mathbb{A}$ by $\mathbb{K} = \mathbb{F}(T)$. One of the valuations $|\cdot|_\infty$ on $\mathbb{K}$, the "infinite" valuation, is induced by the degree map: for $\alpha, \beta \in \mathbb{A}$, define

$$|\alpha/\beta|_\infty = p^{\deg \alpha - \deg \beta}.$$

We let $\mathbb{K}_\infty$ denote the completion of $\mathbb{K}$ with respect to $|\cdot|_\infty$; one easily sees that

Received 21 September 1992. Revision received 2 February 1993.
Walling partially supported by NSF grant DMS 9103303.