Vol. 78, No. 2 DUKE MATHEMATICAL JOURNAL © May 1995

SUPERSINGULAR REDUCTION OF DRINFEL'D MODULES

CHANTAL DAVID

Introduction. Let $R = \mathbb{F}_q[T]$ and $F = \mathbb{F}_q(T)$ be, respectively, the ring of polynomials and the field of rational functions in one indeterminate over the finite field $\mathbb{F}_q$, q a power of an odd prime.

Let ϕ be a rank-2 Drinfel'd R-module defined over $\mathbb{F}_q(T)$. For $p \in \mathbb{F}_q[T]$, a prime of good reduction for ϕ, let ϕ_p denote the reduction of ϕ at p; ϕ_p is then a rank-2 Drinfel'd R-module over the finite field

$$\mathbb{F}_{(p)} = \mathbb{F}_q[T]/(p) \simeq \mathbb{F}_{q^{\deg p}}.$$

Depending on the structure of the endomorphism ring $\mathrm{End}(\phi_p)$, the Drinfel'd module ϕ_p is said to be ordinary or supersingular (see Section 2). Let

$$P(x) = \{\text{monic prime polynomials } p \in \mathbb{F}_q[T]\colon |p| = q^{\deg p} \leqslant x\}.$$

In this paper, we investigate the asymptotic behavior of

$$\pi_\phi(x) = \#\{p \in P(x)\colon \phi \text{ has good supersingular reduction at } p\}.$$

A quadratic extension K/F is said to be imaginary if the prime at infinity does not split in K/F. We say that a Drinfel'd module ϕ has complex multiplication by an order $\mathcal{O}$ of a quadratic imaginary extension K/F if $\mathcal{O} \simeq \mathrm{End}(\phi)$. In this case, by Deuring's criterion (Theorem 2.2) and the Čebotarev density theorem (Theorem 5.1), we get that

(i) when $K \neq F(\sqrt{u})$, u a nonsquare in $\mathbb{F}_q^*$,

$$\pi_\phi(x) \sim \frac{1}{2}\frac{\bar{x}}{\log_q \bar{x}},$$

where $\bar{x}$ is the largest power of q smaller than or equal to x;

(ii) when $K = F(\sqrt{u})$, u a nonsquare in $\mathbb{F}_q^*$,

$$\pi_\phi(x) \sim \frac{\bar{x}}{\log_q \bar{x}}$$

where $\bar{x}$ is the largest *odd* power of q smaller than or equal to x.

Received 7 February 1994.
Author partially supported by CICMA.