ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

THE DISTRIBUTION OF RATIONAL POINTS ON A CURVE DEFINED MODULO Q

R. A. SMITH

1. Introduction. Let f be a polynomial defined over $\mathbf{Z}$ in two variables of total degree $d \geqq 2$, and let $V_p = \{\mathbf{x} \in C_p: f(\mathbf{x}) \equiv 0 \bmod p\}$ for each prime p, where $C_p = \{(x, y) \in \mathbf{Z}^2: 0 \leqq x, y < p\}$. For each subset B in C_p, let $N_p(B) = \text{card } (B \cap V_p)$ and $N_p = \text{card } V_p$. If B is a box in C_p, that is,

$$B = \{(x,y) \in C_p: h < x \leqq h + H, k < y \leqq k + K\},$$

where $0 \leqq h < h + H \leqq p$ and $0 \leqq k < k + K \leqq p$, it is known that (cf. [2], [12])

$$\left|N_p(B) - \frac{|B|}{|C_p|} N_p\right| \leqq 4 \ln^2 p \max_{\mathbf{u} \in C_p^*} |S_p(\mathbf{u})|, \tag{1}$$

where $C_p^* = C_p - \{\mathbf{0}\}$ and $S_p(\mathbf{u})$ is the exponential sum defined by

$$S_p(\mathbf{u}) = \sum_{\mathbf{x} \in V_p} e_p(\mathbf{u} \cdot \mathbf{x}), \tag{2}$$

with $e_p(t) = \exp(2\pi it/p)$. For simplicity, we shall assume that f is absolutely irreducible modulo p for all sufficiently large p, and so, by Weil's well-known result [14],

$$N_p = p + 0(p^{1/2}). \tag{3}$$

Furthermore, we know, by Bombieri [1] (or Chalk and Smith [4]), that

$$|S_p(\mathbf{u})| \leqq (d^2 + 2d - 3)p^{1/2} + d^2 \tag{4}$$

for each $\mathbf{u} \in C_p^*$. If we substitute these results into (1), we obtain

$$N_p(B) = \frac{|B|}{p} + O(p^{1/2} \ln^2 p), \tag{5}$$

for all sufficiently large p. (All O-terms are independent of p, though the inherent constant depends upon d; the same holds for the Vinogradov symbols $\ll$ and $\gg$.) This result shows that the zeros of $f(x,y)$ modulo p

Received by the editors July 4, 1983. . .