76. *Counting Points in a Small Box on Varieties*

By Masahiko FUJIWARA
Department of Mathematics, Ochanomizu University

(Communicated by Kôsaku YOSIDA, M. J. A., Oct. 12, 1988)

§1. Let $G_i(X_1, \cdots, X_n)$ $i=1,2,\cdots,s$ be forms with rational integer coefficients of degree ≥ 2 and $n\geq 4$. Let p be a prime and Q a box in $\boldsymbol{R}^n$, $Q=\{\boldsymbol{x}\in\boldsymbol{R}^n\,;|x_i-a_i|<B_i\ \ i=1,\cdots,n\}$. Consider a system of congruences

$$G_i(X_1,\cdots,X_n)\equiv 0 \pmod p \qquad i=1,\cdots,s.$$

We are interested in the number of solutions $\boldsymbol{x}=(x_1,\cdots,x_n)$ of these congruences, lying in a given relatively small box Q in $\boldsymbol{R}^n$. We write $N(G_1,\cdots,G_s,Q)$ or $N(\boldsymbol{G},Q)$ briefly for that number. Namely,

$$N(\boldsymbol{G},Q)=\#\{\boldsymbol{x}\in\boldsymbol{Z}^n\cap Q\,;\boldsymbol{G}(\boldsymbol{x})\equiv 0 \pmod p\}.$$

In case $Q=[0,p)^n$, there is a classical theorem of Lang and Weil [10] and a far-reaching result of Deligne [6] for nonsingular $\boldsymbol{G}$. When solutions in a small box Q are considered, a delicate handling is required since there are no nontrivial solutions at all if Q is too small; $X_1^d+\cdots+X_n^d\equiv 0 \pmod p$, d even, has nontrivial solutions only if $\max|x_i|\gg p^{1/d}$. G. Meyerson [12] and R. C. Baker [1] gave sufficient conditions for $N>1$. On the other hand W. M. Schmidt [5], though not explicitly mentioned, virtually showed that, under certain nonsingularity condition, $N\sim|Q|/p^s$ for a cube Q of size $\gg p^{1/d+\rho_n(d)}$, where $|Q|$ is the volume of Q and $\rho_n=c_1(d)s/n$. He proved this by using his deep result on "incomplete" exponential sums. His result is in a sense best possible. However, n must be very large in order that the theorem is meaningful, since $c_1(d)$ is very large at present. W. M. Schmidt [15] also gave a condition of similar type for $N\sim|Q|/p^s$, without nonsingular condition. For these, an excellent reference is [2].

In the present paper, we first show that, under some conditions, $N\sim|Q|/p^s$ for any large box Q and $n\geq 4$ (Theorem 1). Throughout our paper, nonsingular mod p means nonsingular over the algebraic closure of the finite field with p elements. Let us introduce the following property $P_G(p)$.

$P_G(p)$: the highest degree part of $a_1G_1+\cdots+a_sG_s$ is nonsingular mod p for all non-zero s-tuples $(a_1,\cdots,a_s)$ of integers (mod p).

Theorem 1. (a) *Let p be a prime, $p\geq B_1,\cdots,B_n\geq c(n,\boldsymbol{d},\varepsilon)$ and $|Q|\geq c(n,\boldsymbol{d},\varepsilon)p^{(n/2)+s}$. Assume that $\boldsymbol{G}$ defines a variety of* codim s mod p *and that $P_G(p)$ holds. Then*

$$(1)\qquad (1-\varepsilon)(|Q|/p^s)\leq N(\boldsymbol{G},Q)\leq(1+\varepsilon)(|Q|/p^s).$$

(b) *Let p be a prime, $p\geq c(n,\boldsymbol{d},\varepsilon)$ and Q a cube with $|Q|\geq p^{(n/2)+s-((n-2s)/(2n-2))}$. Assume that $\boldsymbol{G}$ defines a nonsingular variety of* codim s mod p *and that $P_G(p)$ holds. Then* (1) *holds.*

The proof uses a counting function $F(X)$ introduced later and some