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

Fourier analysis with Deligne's theorem. We remark here that Theorem 1 generalizes the above-mentioned theorems of G. Meyerson and R. C. Baker. We also note that, $n \geq 4$ suffices above, whereas n should exceed $2^{d+1}(d+1)!\,s$ in order that Schmidt's theorem should imply (1) for our box Q. The total number of solutions $\boldsymbol{G}(\boldsymbol{x}) \equiv 0 \pmod{p}$ is usually $\sim p^{n-s}$ and the expectation for these solutions to fall in a box Q is $\sim |Q|/p^n$. Hence, our theorem implies that the rational points of the varieties over finite fields, under a certain nonsingularity condition, are fairly uniformly distributed. We note also that Theorem 1 has any meaning only when $n > 2s$.

Now we consider the property $P_G(p)$. For $s=1$, this is nothing but nonsingularity mod p. However, for $s>1$, even the existence of forms of equal degrees for which $P_G(p)$ holds is not obvious. Some examples for $s=2$ have been given in [15]. How often is this arithmetical condition $P_G(p)$ satisfied? We first introduce a terminology. For positive integers $n, d_1, \cdots, d_s$ and r, let $S(n, \boldsymbol{d}, r)$ be the set of s-tuples of forms of respective degrees $d_1, \cdots, d_s$ with heights $\leq r$ in $\boldsymbol{Z}[X_1, \cdots, X_n]$. We say "for almost all s-tuples of forms of degree $\boldsymbol{d}$" in the sense "for all s-tuples of forms in $S(n, \boldsymbol{d}, r)$ with $0(|S(n, \boldsymbol{d}, r)|^{1-\delta})$ exceptions, where 0 and $\delta > 0$ are independent of r". Our theorem on $P_G(p)$ is the following.

Theorem 2. *Let $G_1, \cdots, G_s$ be forms of degrees d in $\boldsymbol{Z}[X_1, \cdots, X_n]$.*

(a) $s=2$. *For almost all G_1 and G_2, there exists a set of primes with positive density such that, for any p of the set, $P_G(p)$ holds.*

(b) $s \geq 3$. *For almost all $G_1, \cdots, G_s$, $P_G(p)$ is not true for all but a finite number of primes p.*

This theorem states that $P_G(p)$ is often satisfied when $s=1$ or 2, but not when $s \geq 3$, (b) might be rather unexpected since $P_G(p)$ was supposed to be fairly common [15]. The proof relies on resultant theory together with Bertini's theorem, Hilbert irreducibility theorem and Chebotarev density theorem.

Let us turn our attention to the number $N'(\boldsymbol{G}, Q)$ of integer solutions of $\boldsymbol{G}(\boldsymbol{X})=0$ in a given box Q in $\boldsymbol{R}^n$. Namely,

$$N'(\boldsymbol{G}, Q) = \#\{\boldsymbol{x} \in \boldsymbol{Z}^n \cap Q\,;\, G_1(\boldsymbol{x}) = \cdots = G_s(\boldsymbol{x}) = 0\}.$$

The following Theorem 3 generalizes our previous result [7] to simultaneous forms. This theorem is, as was Theorem 1, meaningful only when $n > 2s$. In the following, we call a box Q slim if some side of Q is <1 or $> |Q|^{2/(n+2s)}$. Obviously cubes are not slim.

Theorem 3. (a) *Suppose $G_1, \cdots, G_s$ define a variety of* codim s. *Assume also that there exists a set of primes with positive density such that $P_G(p)$ holds for any p of the set. Then*

$$N'(\boldsymbol{G}, Q) \leq c(n, \boldsymbol{d})\,|Q|^{n/(n+2s)},$$

provided that Q is not slim and $|Q|$ large.

(b) *Suppose furthermore that $\boldsymbol{G}$ is nonsingular over $\boldsymbol{C}$. Then, for any large cube of size B,*

$$N'(\boldsymbol{G}, Q) \leq c(n, d) B^{n-2s+((4s^2-2s)/(n+2s-2))}.$$

We remark here that, in (b), our estimate is better than the trivial estimate B^{n-s} as long as $n>2s$. Our estimate becomes close to the conjectural best bound B^{n-2s} as n becomes large compared with s.

In view of Theorem 2, we can easily prove the following corollaries.

Corollary 1. (a) *Suppose $G_1, \cdots, G_s$ define a variety of* codim s. *Assume each G_i's are nonsingular and have distinct degrees. Then,*

$$N'(\boldsymbol{G}, Q) \leq c(n, \boldsymbol{d})\,|Q|^{n/(n+2s)},$$

provided that Q is not slim and $|Q|$ large.

(b) *Suppose furthermore that $\boldsymbol{G}$ is nonsingular over $\boldsymbol{C}$. Then, for any large cube of size B,*

$$N'(\boldsymbol{G}, Q) \leq c(n, \boldsymbol{d}) B^{n-2s+((4s^2-2s)/(n+2s-2))}.$$

Corollary 2. (a) *Suppose G is nonsingular over $\boldsymbol{C}$. Then*

$$N'(G, Q) \leq c(n, d)\,|Q|^{n/(n+2)},$$

provided that Q is not slim and $|Q|$ large.

(b) *If in particular Q is a large cube of size B, then*

$$N'(G, Q) \leq c(n, d) B^{n-2+(2/n)}.$$

Corollary 3. (a) *For almost all forms G_1, G_2 of degrees d_1, d_2,*

$$N'(\boldsymbol{G}, Q) \leq c(n, d)\,|Q|^{n/(n+4)},$$

provided that Q is not slim and $|Q|$ large.

(b) *If in particular Q is a large cube of size B, then*

$$N'(\boldsymbol{G}, Q) \leq c(n, d) B^{n-4+(12/n+2)}.$$

We remark here that Corollary 2–(b) is nothing but our previous result [7] except for the effective constants there. It should be noted that our method does not allow us to obtain a similar result to Corollary 3 for $s \geq 3$, since $P_G(p)$ fails for almost all $\boldsymbol{G}$ and almost all p's by virtue of Theorem 2.

§ 2. An outline of the proofs. In the proof of Theorem 1, the following "counting function" $F(X)$ plays an important role.

$$F(X) = \begin{cases} 2^n \prod_{i=1}^{n} (1-|X_i|) & \text{if } |X_i| \leq 1 \quad i=1, \cdots, n \\ 0 & \text{otherwise.} \end{cases}$$

In the following, we write $|Q|$ for the volume of $Q=\{\boldsymbol{x} \in \boldsymbol{R}^n ; |x_i - a_i| < B_i \ i=1, \cdots, n\}$ and, for n-dimensional vectors $\boldsymbol{x}=(x_1, \cdots, x_n)$ and $\boldsymbol{B}=(B_1, \cdots, B_n)$, we write $\boldsymbol{B}^{-1}\boldsymbol{x}=(B_1^{-1}x_1, \cdots, B_n^{-1}x_n)$. The next lemma shows that, under some conditions.

$$N(\boldsymbol{G}, Q) \sim \sum_{\substack{x \in \boldsymbol{Z}^n \\ p \mid G(x)}} F(\boldsymbol{B}^{-1}(\boldsymbol{x}-\boldsymbol{a})).$$

Lemma 1. *Assume that, for any prime p and a box* (*resp. a cube*) *Q satisfying $p \geq B_1, \cdots, B_n \geq c_1(n, \boldsymbol{d}, \varepsilon)$ and $|Q| \geq c_1(n, \boldsymbol{d}, \varepsilon) p^\alpha$, the following holds.*

$$(1-\varepsilon)\frac{|Q|}{p^s} \leq \sum_{\substack{x \in \boldsymbol{Z}^n \\ p \mid G(x)}} F(\boldsymbol{B}^{-1}(\boldsymbol{x}-\boldsymbol{a})) \leq (1+\varepsilon)\frac{|Q|}{p^s}.$$

Then, for any prime p and a box (*resp. a cube*) *Q satisfying $p \geq B_1, \cdots, B_n \geq c_2(n, \boldsymbol{d}, \varepsilon)$ and $|Q| \geq c_2(n, \boldsymbol{d}, \varepsilon) p^\alpha$, the following holds.*

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

Using Lemma 1 and Deligne's estimate on exponential sums [6], together with Poisson summation formula, Theorem 1 can be proved. In the proof of Theorem 2, the key is the following lemma.

Lemma 2. *Suppose that G is a form of degree d over K,*

$$G(X_0, \cdots, X_n)=\sum_{i_0+\cdots+i_n=d} a_{i_0\cdots i_n}X_0^{i_0}\cdots X_n^{i_n}, \qquad (a_{i_0\cdots i_n}\in K).$$

Then, there exists a form R of degree >1 with integral coefficients in variables $A_{i_0\cdots i_n}$ $(i_0+\cdots+i_n=d)$, irreducible over $\boldsymbol{C}$, such that G is singular over $\bar{K}$ if and only if $R(a_{i_0\cdots i_n})=0$ in K. Moreover, this R is independent of the field K in the sense that if char $K=0$, *it is a fixed form with integer coefficients; while if* char $K=p(\neq 0)$, *it is obtained by reducing the integer coefficients modulo p.*

The well known resultant satisfies all the properties of Lemma 2 except for absolute irreducibility. Therefore the crucial point of the lemma lies in the absolute irreducibility. We prove that this resultant is a power of some absolutely irreducible form. The proof uses classical algebraic geometry [17]. On the other hand, the proof of Theorem 2 involves Bertini theorem [8], Hilbert irreducibility theorem [11] and Chebotarev density theorem (§3, Chapter 8, [4]). Theorem 3 is proved as an application of Theorem 1. Corollaries 1 and 2 are almost immediate consequences of Theorem 3. The proof of Corollary 3 relies on Theorem 2 and Theorem 3. The details of proofs will appear elsewhere.

References

[1] R. C. Baker: Mathematika, **30**, 164–188 (1983).
[2] ——: Oxford Science Publications. Clarendon Press, Oxford (1986).
[3] B. J. Birch: Mathematika, **4**, 102–105 (1957).
[4] J. W. S. Cassels and A. Fröhlich: Algebraic Number Theory. Academic Press, London (1967).
[5] S. D. Cohen: Proc. London Math. Soc., (3) **43**, 227–250 (1981).
[6] P. Deligne: Publ. Math. IHES., **43**, 273–307 (1973).
[7] M. Fujiwara: Number Theory and Combinatroics (eds. Akiyama *et al.*). World Sci. Publ., Hong Kong, pp. 89–96 (1985).
[8] R. Hartshorne: Algebraic Geometry. Springer, New York (1977).
[9] D. R. Heath-Brown: Proc. London Math. Soc., (3) **47**, 225–257 (1983).
[10] S. Lang and A. Weil: Amer. J. Math., **76**, 819–827 (1954).
[11] S. Lang: Fundamentals of Diophantine Geometry. Springer, New York (1983).
[12] G. Meyerson: Mathematika, **28**, 153–159 (1981).
[13] W. M. Schmidt: Lecture Notes in Math., vol. 536, Springer, Berlin (1976).
[14] ——: Analytische Methoden für Diophantische Gleichungen. DMV Seminar Band 5, Birkhäuser (1984).
[15] ——: Diophantine Analysis (eds. J. H. Loxton and A. J. Van der Poorten). Cambridge University Press (1986).
[16] ——: Mh. Math., **102**, 27–58 (1986).
[17] B. L. Van der Waerden: Grundl. der Math. Wiss., Dover, New York (1945).