

Distribution of integral points on varieties

お茶の水大学 藤原正彦

(Masahiko FUJIWARA)

次の合同式を考える。

$$G_i(X_1, \dots, X_n) \equiv 0 \pmod{p} \quad (i=1, \dots, A)$$

ただし p は素数、 G_i は 整係数の form で 次数 ≥ 2 , $n \geq 4$
 ここで我々が考察するのは、 $\mathbb{R}^n$ に含まれる比較的に小さな箱 Q にある整数解の個数についてである。すなわち、

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

$Q = [0, p)^n$ にとった時は、 $\underline{G} \equiv 0 \pmod{p}$ の個数に
 他ならず、古典的な Lang-Weil (1964) の結果がある。

すなわち、

$G_1, \dots, G_A$ が $\text{codim } s$ の variety を定義している時は、

$$|N - p^{n-s}| < C p^{n-s-\frac{1}{2}}$$

ただし $C = C(n, A, d_1, \dots, d_A)$ は p に無関係。

$\underline{G}$ が $\mathbb{Z}$ 上に non-singular mod p (すなわち、 $\mathbb{Z}/p$ の代数
 的閉包の上で non-singular) ならば、

$$|N - p^{n-1}| < C p^{\frac{n-1}{2}}$$

という Deligne (1974) の結果がある。

Q が $[0, p)^n$ より小さい時はどうだろうか。たとえば

① $G(\underline{x}) = x_1^d + \dots + x_n^d$ (d even) の時、

$$G(\underline{x}) \equiv 0 \pmod{p}, \underline{x} \neq 0 \Rightarrow |\underline{x}| \gg p^{\frac{1}{d}} \text{ だから、}$$

$$Q \text{ を長さ } B \text{ の立方体とすると } B \gg p^{\frac{1}{d}} \text{ となる。}$$

② $G(\underline{x}) = (x_1^2 + \dots + x_n^2)^{\frac{d}{2}}$ (d even) の時、

$$G(\underline{x}) \equiv 0 \pmod{p}, \underline{x} \neq 0 \Rightarrow |\underline{x}| \gg p^{\frac{1}{2}} \text{ だから、}$$

$$B \gg p^{\frac{1}{2}} \text{ となる。}$$

すなわち、 Q を立方体とした時でさえ、 $[0, p)^n$ と比べて小さくし過ぎると、その中に $G \equiv 0$ の解が一つも入らなくなる可能性があるのである。

この論の中で、 $G = 0$ は常に $\text{codim } n$ の variety を定義すると仮定する。また、いつも通り、 $e_p(\alpha) = \exp\left(\frac{2\pi i \alpha}{p}\right)$ と

する。また、 $Q = \{\underline{x} \in \mathbb{R}^n; |\underline{x} - \underline{a}_0| < B\}$ とする。

ここで次の定義をする。

$\underline{G}$ が $P(p, k)$ を満たすとは、次が成立つこととする。

$$\exists c(\underline{G}) \quad \forall \underline{u} \not\equiv 0 \pmod{p} \\ \sum_{\substack{y=0 \\ p \nmid \underline{G}(\underline{y})}}^{p-1} e_p(\underline{u} \cdot \underline{y}) < c(\underline{G}) p^{n-k}$$

左辺の trivial estimate は $e_p(\cdot) = 1$ とした時、右辺は解の個数、可なり $k = n$ となる。従って、 $k \geq n$

(Th.) $\underline{G}$ が $P(p, k)$ を満たすとする。この時、

$$\textcircled{1} \quad \forall B_1, \dots, B_n > \exists c(n, d, \varepsilon), |Q| > \exists c'(n, d, \varepsilon) p^{n+k}$$

となるような箱 Q に対し、ある ε は、

$$\textcircled{2} \quad \text{一辺が } B \geq p^{\frac{n+k}{2}} \text{ なる立方体 } Q \text{ に対し、}$$

$$N(\underline{G}, Q) \sim \frac{|Q|}{p^n}$$

が成立つ。ただし $|Q|$ は Q の体積。

(注) $\underline{G} \equiv 0 \pmod{p}$ の解の個数 $\sim p^{n-k}$ だから、もし

これらが均等に分布しているとする、 Q 内に入る解の

個数は $p^{n-k} \cdot \frac{|Q|}{p^n} = \frac{|Q|}{p^k}$ である。可なり、上の

定理は、 $\underline{G} \equiv 0 \pmod{p}$ の解がかなり均等に分布し

$\Delta = 1$ の時には、他にも、 G absolutely irreducible
 Δ 時、 $N' < c B^{n-\frac{3}{2}} \log B$ (S.D. Cohen 1981),
 G が m -次式を因子に持たない時、 $N' < c B^{n-1-\frac{1}{m-1}} (\log B)^{2n}$
 (Heath-Brown 1983), $G \neq (n-3)$ cylinder の
 時、 $N' < c B^{n-1-\frac{5}{9}}$ (Schmidt 1986), G が
 non-singular の時、 $N' < c B^{n-2+\frac{2}{n}}$ (FUJIWARA 1985)
 , などの結果がある。 G がある条件を満たし、 n が
 非常に大の時には、Hardy-Littlewood の方法が用いら
 れ、 $N' \sim B^{n-d}$ となる。

一般の G について、best bound ほどの位だろうか。

$$G = X_1 X_2^2 + X_3 (X_4^2 + X_5^2 + \dots + X_n^2)$$

とすると、 $x_1 = x_3 = 0$, $x_2, x_4, \dots, x_n$ 任意 であり
 から、 $N' \geq B^{n-2}$ 。 従って、 $n-2$ より小さく

なることは存しない。 一方 $G = X_1 X_2 - X_3 X_4$

の解は $N' \sim B^2 (\log B)^2$

があるから、best bound は、 $B^{n-2} (\log B)^*$

ではないかと Serre は $\frac{1}{2} > \epsilon$ といふ。

(予想) $\text{codim } \Delta$ の variety を定義する G に対して $(d_i \geq 2)$

$$N' < B^{n-2\Delta} (\log B)^*$$

は妥当かも知れない。

(Th.) $\mathbb{Q} - \mathbb{R}$ が B の $\mathbb{Z}$ 分体。 $\underline{G}$ は 密度 > 0 の素数
に対し $I(p, k)$ が成り立つとする。このとき、

$$N'(\underline{G}, B) < c(n, \underline{d}) B^{n-2\rho + \frac{n\rho+2\rho^2-2\rho k}{n+\rho-k}}$$

証明は、FUJIWARA [4] と同様に進めばよい。

(例) ① $\underline{G}$ linearly nonsingular mod p for primes of
positive density, $d_i \geq 2$

$$\Rightarrow N'(\underline{G}, B) < c B^{n-2\rho + \frac{4\rho^2}{n+2\rho}}$$

例えば、 $d_i \geq 2$ 且 distinct, $\forall G_i$ nonsingular
なら linearly nonsingular for almost all p となる
で、上の評価が成立する。

証明は、FUJIWARA [4]

② $\underline{G}$ nonsingular, complete intersection, $d_i \geq 2$

$$\Rightarrow N'(\underline{G}, B) \leq c B^{n-2\rho + \frac{2\rho^2}{n+\rho-1}}$$

証明は Shparlinskii - Skorobogatov [9]。 $\rho=1$ の

時は $N' \leq c B^{n-2+\frac{2}{n}}$ となるが、この証明は、

FUJIIWARA [] にある。

③ $\underline{G}$ に l 個の linear form が λ である時は、上の①, ②は成立せず、次のようになる。

① で $l > 0$ の linear form が λ である時、

$$N' \leq B^{n-2\lambda+l} + \frac{4(\lambda-l)^2}{n+2\lambda-3l}$$

② で $l > 0$ の linear form が λ である時、

$$N' \leq B^{n-2\lambda+l} + \frac{2(\lambda-l)^2}{n+\lambda-2l-1}$$

(注) ③ で、 $\lambda = l$ (すなわち λ 個の linear form)

の時は、どちらも $N' \leq B^{n-l}$ となり、当然と

なる。また $l = 0$ の時は、①, ②と同様に成る

ことから、当然の一般化と言えよう。

References

- [1] S.D. Cohen. The distribution of Galois groups and Hilbert irreducibility theorem. Proc. London Math. Soc. (3), 43 (1981) 227-250
- [2] P. Deligne. La conjecture de Weil I. Publ. Math. IHES., 43 (1974), 273-307
- [3] M. FUJIMURA. Upper bounds for the number of lattice points on hypersurfaces. Number Theory and Combinatorics, edit. by Akiyama et al. (World Sci. Publ., Hong Kong, 1985), 89-96
- [4] " . Distribution of rational points on varieties over finite fields. Mathematika, Part 2 Vol 35 (1988), 155-171
- [5] " . Counting points in a small box on varieties, Proc. of the Japan Acad. Ser. A No. 8 vol 64 (1988), 267-270

- [6] D. R. Heath-Brown, Cubic forms in 10 variables,
Proc. London Math. Soc. (3), 47 (1983), 225-257
- [7] W. M. Schmidt, Small solutions of congruences,
Diophantine Analysis, edit. by J. H. Loxton, A. J. Van
der Poorten (Cambridge University Press, 1986).
- [8] . Integer points on hypersurfaces,
Mh. Math., 102 (1986), 27-58
- [9] Shparlinskii, Skorobogator, Exponential sums and
rational points on complete intersections, Matematika
37 (1990)