ON SOLUBILITY OF DIOPHANTINE EQUATIONS (A SURVEY OF SOME RESULTS FROM THE ANALYTIC THEORY OF NUMBERS)

B.Z.Moroz

1.Introduction. [1]

Denoting by $x := (x_1, \ldots, x_n)$ a set of n independent variables, let

$$g = (g_1, \ldots , g_r),\ g_j(x) \in \mathbb{Z}[x],\ 1 \leq j \leq r,$$

and let d_j denote the degree of the polynomial g_j; without loss of generality, we may assume that $d_j \geq 2$, $1 \leq j \leq r$, and $n > r$. The systems of Diophantine equations of the form

$$g(x) = 0 \tag{1}$$

fall into three groups: (I) those soluble in $\mathbb{Z}$, (II) those (ZF-) provably insoluble in $\mathbb{Z}$, and (III) those insoluble in $\mathbb{Z}$ equations, whose insolubility can not be proved. The analytic methods of classical number theory allow one to describe some classes of (systems of) Diophantine equations contained in $(I) \cup (II)$, in that an equation in a given class is proved to be soluble if it satisfies certain necessary conditions of solubility (for instance, if it is soluble in $\mathbb{R}$ and in $\mathbb{Z}_p$ for each prime p).

A class of Diophantine equations is said to be decidable if there is an algorithm to determine solubility in $\mathbb{Z}$ of an arbitrary equation in this class. The set $(II) \cup (III)$ is trivially decidable, the set $(I) \cup (II)$ is also decidable; in view of the negative solution of the Hilbert's tenth problem (cf. [4]), the set $(I) \cup (III)$ is undecidable. One should also note that the set (III) is, of course, not a listable set. It is an outstanding open problem to determine whether the class of all the *homogeneous* Diophantine equations be decidable. After the work of Minkowski, Hasse, Siegel, and Watson, the class of quadratic equations is known to be decidable; F.J. Grunewald and D. Segal [5] describe the corresponding algorithm in detail. On the other hand, an easy (and well - known) argument shows that there is a system of quadratic equations, or what amounts to the same thing an equation of degree 4, whose solubility in $\mathbb{Z}$ is equivalent to solubility of the given Diophantine equation. Moreover, there is a Diophantine equation $g(x)z^m + z^2 - 1 = 0$ of degree $4 + m, m > 0$, soluble in $\mathbb{Z}$ if and only if the fourth degree equation $g(x) = 0, g(x) \in \mathbb{Z}[x]$, is soluble in $\mathbb{Z}$. In particular, if $l > 3$, the set of Diophantine equations of degree l is undecidable, and the set (III) contains a Diophantine equation of degree l (cf. [4]). I do not know whether the set (III) contains a cubic Diophantine equation, let alone if the class

[1] This is a corrected and slightly edited version of my MPIM Preprint, 118(1999).

of cubic Diophantine equations be undecidable. Is the class of homogeneous cubic Diophantine equations decidable? We shall return to the problem of solubility of cubic equations in $n°4$.

As usual, $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$, and $\mathbb{Z}_p$ denote the sets of complex numbers, real numbers, rational numbers, rational integers, and p-adic integers, respectively; p ranges over the rational primes.

2.The Hardy-Littlewood circle method.

Introduced in a paper of Hardy and Ramanujan in 1918 and developed in the classic series of papers "Some problems of Partitio Numerorum" (1920-1928) by Hardy and Littlewood, the circle method remains an important tool in studying Diophantine equations. The recent monograph [13] and the survey article [10] contain an extensive bibliography of numerous works, relating to this method and its applications in number theory; one may also wish to consult the recent memoir [7] on a new form of this method, and the survey [2] on the "adelic" version of the circle method.

The circle method is designed to give an asymptotic formula for the number

$$\mathcal{N}(t) = \mathrm{card}\{a \mid a \in t\,\mathfrak{B}, g(a) = 0, a \in \mathbb{Z}^n\}$$

of integer solutions of the equation (1) contained in the subset $t\mathfrak{B}$ of $\mathbb{R}^n$, as $t \to \infty$, where $\mathfrak{B}$ is a fixed convex subset of $\mathbb{R}^n$.

Let $T = (S^1)^r$ be an r-dimensional torus, and let

$$w(\alpha) = \sum_{a \in t\mathfrak{B} \cap \mathbb{Z}^n} e^{2\pi i \alpha g(a)}$$

for $\alpha \in T$; clearly, $\mathcal{N}(t) = \int_T w(\alpha)\, d\alpha$. For $\beta \in \mathbb{R}$, let $\|\beta\| := \min_{m \in \mathbb{Z}} |\beta - m|$. One divides T into two subsets, the *major arcs*

$$\mathfrak{M} = \{\alpha \mid \alpha \in T, \exists\, q \in \mathbb{Z}\,(\,1 \le q \le t^\delta \text{ and } \|q\alpha_j\| \le t^{-d_j+\delta}, 1 \le j \le r)\},$$

and the *minor arcs* $\mathfrak{m} = T \setminus \mathfrak{M}$, the parameter $\delta \ge 0$ being adjusted in the course of calculations. It follows that

$$\mathcal{N}(t) = I(\mathfrak{M}) + I(\mathfrak{m})$$

with $I(U) := \int_U w(\alpha)\, d\alpha$ for a (measurable) subset U of T. The circle method is said to *work* if

$$I(\mathfrak{M}) = \mu\, t^{n-D}(1 + o(1)), \text{and}\, I(\mathfrak{m}) = o(t^{n-D})$$

with $D := \sum_{1 \le j \le r} d_j$ and $\mu = \mu(\infty)\mu_0$, where $\mu(\infty)$ and μ_0 stand for the *singular integral* and the *singular series* respectively; moreover, it *works well* if it works with $\mu > 0$. To define the singular series, let $\mathcal{P}$ denote the set of rational primes, suppose that the "local density " of solutions

$$\mu_p = \lim_{l \to \infty} p^{l(r-n)} \mathrm{card}\,\{a \mid a \in (\mathbb{Z}/p^l\mathbb{Z})^n, g(a) = 0 \pmod{p^l}\,\}$$

exists for $p \in \mathcal{P}$, and let $\mu_0 = \prod_{p \in \mathcal{P}} \mu_p$. To define the singular integral, write

$$g = f + h, f := (f_1, \ldots, f_r), h := (h_1, \ldots, h_r),$$

where f_j is a homogeneous polynomial of degree d_j and the polynomial h_j is of degree smaller than d_j, $1 \leq j \leq r$, and let $|f(\xi)| := \max_{1\leq j\leq r} |f_j(\xi)|$. By definition,

$$\mu(\infty) = \lim_{L\to\infty} L^r \int_{\xi\in\mathfrak{B},\, L|f(\xi)|\leq 1} \prod_{j=1}^{r}(1 - Lf_j(\xi))\, d\xi.$$

If the circle method works well, one obtains an asymptotic formula

$$\mathcal{N}(t) \sim \mu\, t^{n-D},\ \mu > 0, \tag{2}$$

and, a fortiori, proves that the equation (1) is soluble. The asymptotic formula (2) may still hold, and even be provable by other methods, when the circle method *fails* (:= does not work). Let (I.1) denote the class of those equations (1) which satisfy relations (2) for a suitably chosen set $\mathfrak{B}$, and let (I.2) be the set of the equations (1) satisfying $\mathcal{N}(t) \gg t^{\gamma}$ with $\gamma > 0$ for some $\mathfrak{B}$. Clearly, $(I.1) \subseteq (I.2) \subseteq (I)$, and, moreover, $(I.1) \neq (I.2) \neq (I)$.

3.Two theorems of B.J.Birch.

In the mid-thirties, Tartakovskii applied the circle method to prove solubility of a "generic" equaton (1) for large n. In 1957, Birch proved that a system of homogeneous equations of odd degrees has a non-trivial zero, providing the number of independent variables be big enough; a few years later he obtained another general theorem asserting that the equation (1) is soluble in $\mathbb{Z}^n$, as soon as the codimension of the "singular locus" of the variety, say, V defined by (1) is sufficiently large. We give a modern version of these theorems, following the recent papers [12],[16] (cf. also [17]).

Let us suppose, for simplicity, that $d_1 = \cdots = d_r =: d$. Let $v(3, r) = (10r)^5$, $v(5, r) = \exp(10^{32} r^6 (\log 3r)^7)$, and $v(d, r) = \psi_{(d-5)/2}(dr)$ for $d \geq 7$, assuming d is odd,where $\psi_0(x) = e^x$, and $\psi_l(x) = \psi_{l-1}^{[42 \log x]}(x)$ for $x > 0$ (as usual, $[y]$ stands for the biggest integer $\leq y$). The following variant of the first theorem of Birch is due to T.D.Wooley (for $d \geq 5$), and to W.M.Schmidt (for $d = 3$).

Theorem 1. *Suppose g_j, $1 \leq j \leq r$, be a homogenous polynomial of odd degree d. Then*

$$n \geq v(d, r) \Longrightarrow \exists\, a \in \mathbb{Z}^n\ (\, g(a) = 0 \,\text{and}\, a \neq 0).$$

To state the second theorem of Birch, we require some further notation. Given a polynomial map $q : \mathbb{C}^n \to \mathbb{C}^m$, let V(q) be the affine complex variety defined by the equation $q(x) = 0$; let $\tilde{W}$ stand for the singular locus of the affine complex variety W.[2] Finally, let $\Delta(f)$ be equal to the dimension of the affine complex variety defined by the condition $\operatorname{rank} J(f) < r$, where $J(f) := (\frac{\partial f_j}{\partial x_i})_{\substack{1\leq j\leq r\\ 1\leq i\leq n}}$ stands

[2]For brevity, we write "variety" for what is normally called algebraic set, irreducibility not being thereby implied.

for Jacobian of the map $f:\mathbb{C}^n\to\mathbb{C}^m$. Assuming $\dim V(f)=n-r$, one can prove that $\Delta(f)$ is actually equal to the dimension of the (Zariski-)closure of the union

$$\cup_{\mu\in\mathbb{C}^r}\tilde{V}(f-\mu)$$

of the loci of singularities of the affine varieties defined by the (systems of) equations $f(x)=\mu$, $\mu\in\mathbb{C}^r$, cf. [1].

Theorem 2. *Choose* $\mathfrak{B}=\prod_{j=1}^n[b_j-1/2,b_j+1/2)$, *and suppose that* $n>\Delta(f)+2^{(d-1)}(d-1)r(r+1)$. *Then the circle method works. If, moreover,* $\dim V(f)=n-r$, *then*

$$b\in(V(f)\setminus\tilde{V(f)})(\mathbb{R})\Longrightarrow\mu_\infty>0,$$

where $b:=(b_1,\ldots,b_n)$, *and*

$$\forall p\in\mathcal{P}\,(\,(V(f)\setminus\tilde{V(f)})(\mathbb{Z}_p)\neq\emptyset\,)\Longrightarrow\mu_0>0.$$

In particular, if $n>\Delta(f)+2^{(d-1)}(d-1)r(r+1)$, $\dim V(f)=n-r$, and $\forall p\in\mathcal{P}\,(\,(V(f)\setminus\tilde{V(f)})(\mathbb{Z}_p)\neq\emptyset\,)$, *then the circle method works well as soon as* $b\in(V(f)\setminus\tilde{V(f)})(\mathbb{R})$.

4.Cubic Diophantine equations.

In this section, we review rather old (but rarely cited) results of Davenport, Lewis, and Watson. Let $r=1$ and $d_1=3$, so that $g=f+h$ is a cubic polynomial, f is a cubic form, and h is a quadratic polynomial. Following [3], [14], [15], we let $\nu(g)=\min\{s\mid f=\sum_{i=1}^s l_iq_i$ with linear l_i and quadratic $q_i\}$. Suppose the polynomial g be irreducible and *non-degenerate*, i.e. not equivalent (over $\mathbb{Z}$) to a polynomial of less than n variables. Suppose also the congruence

$$g(x)=0\pmod{p^k}\qquad(3)$$

be soluble for every prime power p^k. Then each of the following three conditions implies solubility of the equation (1) in $\mathbb{Z}^n$:

(i) $\nu(g)\geq 17$;

(ii) $n\geq 15$ and $4\leq\nu(g)\leq n-3$;

(iii)$n\geq 14$, and there is an indefinite quadratic form $q(x_1,\ldots,x_{n-1})$ such that $f(x)=x_nq(x_1,\ldots,x_{n-1})$, the quadratic form $q(x_1,\ldots,x_{n-2},0)$ is positive definite, and equation (1) cannot be put into the shape $(ax_n+b)S(x)=a'x_{n-1}^2+b'x_{n-1}+c'$ except possibly with $a'\neq 0$ and $b'^2-4a'c'$ a square.

Let us remark that each of the conditions (i)-(iii) is decidable, and refer to the original papers [3], [14], [15] for the detailed proof and discussion of the cited results.

Corollary. *If* $n\geq 19$, $\nu(g)\geq 4$, *and the congruence condition* (3) *is satisfied, then the equation* (1) *is soluble in* $\mathbb{Z}^n$.

These results allow us to isolate a big decidable subclass of cubic Diophantine equations. One can hardly expect, however, the whole class of cubic equations be decidable.

The known results concerning solubility of cubic equations in rationals are much easier to state. By an old theorem of Davenport, a *homogeneous* cubic polynomial

f represents zero non-trivially over $\mathbb{Z}$ (or, what amounts to the same thing, over $\mathbb{Q}$) if $n \geq 16$. In the eighties, Heath-Brown proved [6] that every *non-singular* form f represents zero non-trivially over $\mathbb{Z}$ as soon as $n \geq 10$, and Hooley proved [9] the Hasse-Minkowski principle to hold for the class of non-singular cubic forms f with $n \geq 9$.

5.Concluding remarks.

The second theorem of Birch and Davenport's "sixteen variables result" have been proved by an adaptation of the classical circle method. On the other hand, in order to prove the first theorem of Birch and to obtain the results on solubility of non-homogeneous cubic equations, described in $n°4$, the authors supplement the circle method by some elementary, albeit highly non-trivial, considerations. Finally, Heath-Brown's "ten variable result" and Hooley's "nine variable result" have been proved by making use of the variant of the circle method introduced in the work of Kloosterman on quarternary quadratic forms; this form of the circle method allows to incorporate the estimates of exponential sums, obtained as a consequence of the Weil conjectures proved by Deligne.

By the very nature of the circle method, it can not be applied to treat those equations which are insoluble, or do not have enough solutions to fall into the set (I.2). Moreover, there are many difficult Diophantine problems given by equations contained in the set (I.2) which could not be solved by the circle method; I do not attempt to describe the many ingenious methods, which have led to a solution of some of these problems (cf., for instance, [8]).

However, other methods of analytic number theory can be sometimes applied to study Diophantine equations having not too many solutions. For instance, the Birch and Swinnerton-Dyer conjecture, if true, can be used to prove the $\mathbb{Q}$-decidabilty of the set of the elliptic curves; at present, no general algorithm is known to decide, whether an elliptic curve have a rational point, although one can usually answer this question for a given elliptic curve, by one method or another.[3] As an application of A. Baker's estimates of linear forms in logarithms of algebraic integers, one can prove that the class of Thue and superelliptic equations is decidable (cf., for instance, [11]). These problems lie far beyond the scope of this survey, however, and I shall not comment on these questions any further.

A preliminary version of this survey circulated among the participants of the workshop on Hilbert's tenth problem held in Gent (Belgium) during the first week of November 1999. It is a pleasure to thank the organisers of this workshop for their hospitality. I am grateful to Professor G. Cherlin for an interesting and instructive conversation during the conference, and to Professor Yu. V. Matiyasevich for pointing out a mistake in the first version of this paper.

References

1. A.G.Aleksandrov and B.Z.Moroz, Complete intersections in relation to a paper of B.J.Birch, submitted for publication.
2. R.Danset, Méthode du cercle adélique et principe de Hasse fin pour certaines systèmes de formes, L'Enseignement Mathématique, **31** (1985), 1-66.
3. H. Davenport and D.J. Lewis, Non-homogeneous cubic equations, Journal of the London Math. Soc., **39** (1964), 657-671.
4. M. Davis, Yu. Matijasevič, and Ju. Robinson, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, Proc. of Symposia in Pure Maths, **28** (1976), 323-378.

[3] I am obliged to Professor D. B. Zagier for a discussion of this problem, [18].

5. F.J. Grunewald and D. Segal, How to solve a quadratic equation in integers, Math. Proc. of the Cambridge Phil. Soc., **89** (1981), 1-5.
6. D.R. Heath-Brown, Cubic forms in ten variables, Proc. of the London Math. Soc., **47** (1983), 225-257.
7. D.R. Heath-Brown, A new form of the circle method, and its application to quadratic forms, Journal für die reine und angew. Mathematik, **481** (1996), 149-206.
8. C. Hooley, Some recent advances in analytic number theory, Proc. of the ICM 1983, Warszawa, 85-97.
9. C. Hooley, On nonary cubic forms, Journal für die reine und angew. Mathematik, **386** (1988), 32-98.
10. W.M. Schmidt, The density of integer points on homogeneous varieties, Acta Math., **154** (1985), 243-296.
11. T.D. Shorey and R.Tijdeman, Exponential Diophantine equations, Cambridge Tracts in Maths, **87**, Cambridge Univ. Press, 1986.
12. C.M. Skinner, Forms over number fields and weak approximation, Compositio Math., **106** (1997), 11-29.
13. R.C. Vaughan, The Hardy-Littlewood circle method, Cambridge Tracts in Maths, **125**, Cambridge Univ. Press, 1997.
14. G.L. Watson, Non-homogeneous cubic equations,Proc. of the London Math. Soc., **17** (1967), 271-295.
15. G.L. Watson, Cubic Diophantine equations with reducible cubic part, Proc. of the London Math. Soc.,**21** (1970), 181-200.
16. T.D. Wooley, An explicit version of Birch's theorem, Acta Arithmetica, **85** (1998), 79-96.
17. T.D. Wooley, Diophantine problems in many variables: The role of additive number theory, in: Topics in number theory, Maths and its Applications, **467**, Kluwer Acad. Publ. Dordrecht, 1999, p.49- 83.
18. D.B.Zagier, Private communication, Spring 1998.

Max-Planck-Institut für Mathematik, Vivatsgasse 7,D-53111 Bonn, Germany