

A FEW REMARKS RELATING TO THE SOLUBILITY OF DIOPHANTINE EQUATIONS.

B.Z. MOROZ

§1. Some consequences of Matiyasevich's theorem.

1. In 1970, Yu.V. Matiyasevich proved [14] the following remarkable theorem.

Theorem 1. *Every recursively enumerable set is Diophantine.*

Corollary 1. *There is no algorithm deciding whether a given Diophantine equation is soluble in \mathbb{Z} .*

It follows from this result that any recursively enumerable first order theory of Diophantine equations is necessarily incomplete. In this section we comment on that observation and its consequences for the theory of Diophantine equations. It is to be contrasted with the results from the analytic theory of Diophantine equations, discussed in the subsequent sections of this brief survey.

Notation and conventions. As usual, in what follows $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p,$ and \mathbb{N} stand for the field of complex numbers, the field of real numbers, the field of rational numbers, the ring of rational integers, the ring of p -adic integers, and the monoid of positive rational integers respectively; p ranges over the rational primes. We let $PA, ZFC,$ and $ZFCI$ denote the first order Peano Arithmetic, the Zermelo-Fraenkel set theory with the Axiom of Choice, and the "ZFC + {there is an inaccessible cardinal}" respectively. For brevity, we shall write "*variety*" for what is normally called algebraic set, *irreducibility* not being thereby implied.

Let us recall that a subset S of \mathbb{Z} is said to be *recursively enumerable* if there is a recursive function $F: \mathbb{N} \rightarrow \mathbb{Z}$ such that $F(\mathbb{N}) = S$. If both sets S and $\mathbb{Z} \setminus S$ are recursively enumerable, the set S is called *recursive*. For $n \in \mathbb{N}$, let

$$f(t, \vec{x}) \in \mathbb{Z}[t, \vec{x}], \quad \vec{x} := (x_1, \dots, x_n),$$

and let

$$A(f) := \{a \mid a \in \mathbb{Z}, \exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ f(a, \vec{b}) = 0)\}.$$

A subset B of \mathbb{Z} is said to be *Diophantine* if there are n in \mathbb{N} and a polynomial $f(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ such that $B = A(f)$. In view of *Church's thesis* (cf. [20, p. 160]), Corollary 1 follows from Theorem 1 since there exist recursively enumerable sets which are not recursive. As a point of fact, given a recursively enumerable set B , one can actually *construct* a polynomial $f(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ such that $B = A(f)$ (cf. [4, p. 325]); moreover, one can *construct* a polynomial $U(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$, for some n in \mathbb{N} , such that there is no algorithm to determine whether an integer a satisfies the formula

$$\exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ U(a, \vec{b}) = 0),$$

cf. [15, p. 17].

Let \mathcal{T} be a first order theory. We denote by $L(\mathcal{T})$ the language of \mathcal{T} , let $\mathfrak{F}(\mathcal{T})$ be the set of all the formulae in $L(\mathcal{T})$, and let $\mathfrak{T}(\mathcal{T})$ be the set of the theorems of \mathcal{T} . By definition,

$$\mathfrak{T}(\mathcal{T}) \subseteq \mathfrak{F}(\mathcal{T}).$$

We shall assume that there exists an one-to-one map

$$\varphi: \mathfrak{F}(\mathcal{T}) \rightarrow \mathbb{N},$$

a "*canonical*" numbering of $\mathfrak{F}(\mathcal{T})$, such that the set $\varphi(\mathfrak{T}(\mathcal{T}))$ is recursively enumerable. In view of that assumption, one can construct a polynomial $F_{\mathcal{T}}(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ with

$$\varphi(\mathfrak{T}(\mathcal{T})) = A(F_{\mathcal{T}}).$$

Suppose that

$$L(PA) \subseteq L(\mathcal{T}).$$

Moreover, let us assume that a formula of the shape

$$\exists \vec{b} (\vec{b} \in \mathbb{Z}^n \ \& \ f(\vec{b}) = 0),$$

with $f(\vec{x}) \in \mathbb{Z}[\vec{x}]$, is provable in \mathcal{T} if and only if it is *true*; in particular, the theory \mathcal{T} is assumed to be *consistent*. It follows then that there is an infinite sequence of polynomials

$$f_1(\vec{x}), f_2(\vec{x}), \dots$$

such that $f_i(\vec{x}) \in \mathbb{Z}[\vec{x}]$ and the formula

$$\forall \vec{b} (\vec{b} \in \mathbb{Z}^n \rightarrow f_i(\vec{b}) \neq 0)$$

is *true* but *not* provable in \mathcal{T} , for every i ; one could let, for instance,

$$f_i(\vec{x}) = U(a_i, \vec{x}), \quad i = 1, 2, \dots$$

for a suitable sequence of integers a_1, a_2, \dots . Therefore the theory \mathcal{T} is *incomplete*. Assume, moreover, that the theory \mathcal{T} is an *extension* of PA, and let $\mathfrak{C}_{\mathcal{T}}$ be the formula in $L(\mathcal{T})$ stating that \mathcal{T} is consistent. Let

$$\varphi(\mathfrak{C}_{\mathcal{T}}) = a_0$$

and let

$$f_0(\vec{x}) := F_{\mathcal{T}}(a_0, \vec{x}).$$

By Gödel's theorem [20, p. 213],

$$\mathfrak{C}_{\mathcal{T}} \notin \mathfrak{T}(\mathcal{T}).$$

Therefore it follows that the formula

$$(1) \quad \forall \vec{b} (\vec{b} \in \mathbb{Z}^n \rightarrow f_0(\vec{b}) \neq 0)$$

is true but not provable in \mathcal{T} .

On letting $\mathcal{T} = PA$, one obtains a formula of the form (1) which is true but not provable in Peano Arithmetic. Moreover, it is well-known that consistency of ZFC is provable in $ZFCI$; see, for instance, [11, p. 167]. Therefore, on letting $\mathcal{T} = ZFC$, one obtains a formula of the form (1) provable in $ZFCI$, but not in ZFC . The reader may consult the works [12], [5], and references therein for some related results.

2. As above, let $\vec{x} := (x_1, \dots, x_n)$ be a set of n independent variables, let

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

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

$$(2) \quad \vec{g}(\vec{x}) = 0$$

fall into three groups: (I) those soluble in \mathbb{Z} , (II) those \mathcal{T} -provably insoluble in \mathbb{Z} , and (III) those insoluble in \mathbb{Z} equations, whose insolubility can not be proved in \mathcal{T} (cf. [17]). 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 Corollary 1, the set (I) \cup (III) is undecidable. One should also note that (III) is, of course, *not* a recursively enumerable set. 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 [6] 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 the solubility of a system of Diophantine equations of the form (2). 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 of cubic Diophantine equations is undecidable. We shall return to the problem of solubility of cubic equations in §4.

The analytic methods of classical number theory, to be discussed in §2 – §5, allow one to describe some classes of (systems of) Diophantine equations contained in $(I) \cup (II)$, with $\mathcal{T} = ZFC$ say, 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).

3. It is an outstanding open problem to determine whether the class of the *homogeneous* Diophantine equations is decidable.

Lemma 1. *The following two decision problems are equivalent:*

- 1) *the problem of determining the existence of a rational solution for an arbitrary Diophantine equation;*
- 2) *the problem of determining the existence of a non-trivial integer solution for an arbitrary homogeneous Diophantine equation.*

Proof. See [16, §7.4].

Let R be a commutative ring and suppose that $\mathbb{Z} \subseteq R$. For $n \in \mathbb{N}$, let

$$f(t, \vec{x}) \in R[t, \vec{x}], \quad \vec{x} := (x_1, \dots, x_n),$$

and let

$$\mathcal{A}(R, f) := \{a \mid a \in R, \exists \vec{b} (\vec{b} \in R^n \ \& \ f(a, \vec{b}) = 0)\}.$$

A subset S of R is said to be *definable in R* if $S = \mathcal{A}(R, f)$ for some n in \mathbb{N} and a polynomial $f(t, \vec{x})$ in $R[t, \vec{x}]$. Thus a subset B of \mathbb{Z} is Diophantine if and only if B is definable in \mathbb{Z} . The ring R is said to be *universal* if every recursively enumerable subset B of \mathbb{Z} is definable in R . Finally, we say that R is a *real ring* if

$$\sum_{1 \leq j \leq r} a_j^2 = 0 \rightarrow \forall j (a_j = 0)$$

for any \vec{a} in $R^r, r \in \mathbb{N}$.

Corollary 2. (cf. [16, §7.3]) *A real commutative ring R , containing \mathbb{Z} , is universal if and only if \mathbb{Z} is definable in R .*

Proof. If R is an universal ring, then \mathbb{Z} is definable in R since the set \mathbb{Z} is recursively enumerable. Conversely, suppose that

$$(3) \quad \mathbb{Z} = \mathcal{A}(R, f)$$

for some l in \mathbb{N} and a polynomial $f(t, \vec{x})$ in $R[t, \vec{x}]$, $\vec{x} := (x_1, \dots, x_l)$. Let us consider a recursively enumerable subset B of \mathbb{Z} . By Theorem 1, the set B is Diophantine, therefore

$$(4) \quad B = A(g)$$

for some m in \mathbb{N} and a polynomial $g(t, \vec{y})$ in $\mathbb{Z}[t, \vec{y}]$, $\vec{y} := (y_1, \dots, y_m)$. Let

$$(5) \quad F(t, \vec{u}) := g(t, \vec{y})^2 + f(t, \vec{z})^2 + \sum_{1 \leq j \leq m} f(y_j, \vec{x}^{(j)})^2,$$

where \vec{u} stands for the array of $m + l + ml$ independent variables

$$\vec{y}, \vec{z}, \vec{x}^{(j)}, 1 \leq j \leq m.$$

It follows from the relations (3) - (5) that $B = \mathcal{A}(R, F)$. This completes the proof of the corollary.

Open problem. *Is the field \mathbb{Q} universal ?*

This problem lies at the heart of the current research, relating to Hilbert's 10th problem (see, for instance, [19] and references therein). In view of Corollary 2, the field \mathbb{Q} is universal if and only if the ring \mathbb{Z} is definable in \mathbb{Q} . As above, it follows from Church's thesis that if the field \mathbb{Q} is universal, then there is no algorithm deciding whether a given Diophantine equation is soluble in \mathbb{Q} . Therefore, in view of Lemma 1, the class of the homogeneous Diophantine equations is undecidable if the field \mathbb{Q} is universal.

Open problem. *Is the class of the cubic homogeneous Diophantine equations decidable?*

§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 [24] and the survey article [18] 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 [8] on a new form of this method and the survey article [2] on the "adelic" version of the circle method.

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

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

of integer solutions of the equation (2) contained in the subset $t\mathfrak{B}$ of \mathbb{R}^n , as $t \rightarrow \infty$, where \mathfrak{B} is a fixed convex subset of \mathbb{R}^n .

Let $S^1 = \mathbb{R}/\mathbb{Z}$ be the unit circle and let $T = (S^1)^r$ be an r -dimensional torus. Let

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

for $\vec{\alpha} \in T$; clearly,

$$\mathcal{N}(t) = \int_T w(\vec{\alpha}) d\vec{\alpha}.$$

For $\beta \in \mathbb{R}$, let $\|\beta\| := \min_{m \in \mathbb{Z}} |\beta - m|$. One divides T into two subsets, the *major arcs*

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

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

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

with

$$I(U) := \int_U w(\vec{\alpha}) d\vec{\alpha}$$

for a (measurable) subset U of T . Let \mathcal{P} stand for the set of rational primes. Let

$$\vec{g} = \vec{f} + \vec{h}, \vec{f} := (f_1, \dots, f_r), \vec{h} := (h_1, \dots, h_r),$$

where f_j is a homogeneous polynomial of degree d_j and the degree of the polynomial h_j is smaller than d_j , $1 \leq j \leq r$, and let

$$|\vec{f}(\vec{\xi})| := \max_{1 \leq j \leq r} |f_j(\vec{\xi})|.$$

The circle method is said to *work* if the following conditions are satisfied:

- 1) For $p \in \mathcal{P}$, there exists the "local density" of solutions

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

and the infinite product

$$\mu_0 = \prod_{p \in \mathcal{P}} \mu_p$$

converges.

- 2) The integrals $I(\mathfrak{M})$ and $I(\mathfrak{m})$ can be estimated as follows:

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

as $t \rightarrow \infty$, with

$$D := \sum_{1 \leq j \leq r} d_j, \quad \mu = \mu(\infty) \mu_0,$$

where

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

The circle method *works well* if it works with $\mu > 0$. The constants $\mu(\infty)$ and μ_0 are called the *singular integral* and the *singular series* respectively. If the circle method works well, one obtains an asymptotic formula

$$(6) \quad \mathcal{N}(t) \sim \mu t^{n-D}, \mu > 0,$$

and, a fortiori, proves that equation (2) is soluble. The asymptotic formula (6) 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 (2) which satisfy relations (6) for a suitably chosen set \mathfrak{B} and let (I.2) be the set of the equations (2) 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).

Remark. It is hardly possible to give reasonably simple conditions describing the sets (I.1) and (I.2); I do not even know whether those sets are recursively enumerable. Nor seems it possible to describe, in simple terms, the class of the Diophantine equations satisfying condition 1) above.

The circle method, as described above, should be regarded as a highly successful tool for investigating the solubility of certain classes of Diophantine equations. In the next section, we give a simple sufficient condition for the circle method to work (well), see Theorem 3. In the monograph [24], the reader will find several examples of (classes of) Diophantine equations, which have been proved to be soluble by the circle method. Our exposition in this section has been somewhat influenced by the work [18].

§3. Two theorems of B.J.Birch

In the mid-thirties, Tartakovskii applied the circle method to prove solubility of a "generic" equation (2) 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 equation (2) is soluble in \mathbb{Z}^n as soon as the codimension of the "singular locus" of the variety, defined by (2), is sufficiently large. We give a modern version of these theorems, following the recent papers [22], [27] (cf. also [28]).

Let us suppose, for simplicity, that $d_1 = \dots = d_r =: d$. 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 2.. *Suppose g_j , $1 \leq j \leq r$, be a homogenous polynomial of odd degree d . Then*

$$n \geq v(d, r) \rightarrow \exists \vec{a} \in \mathbb{Z}^n (\vec{g}(\vec{a}) = 0 \& \vec{a} \neq 0).$$

To state the second theorem of Birch, we require some further notation. Given a polynomial map $q : \mathbb{C}^n \rightarrow \mathbb{C}^m$, let $V(q)$ be the affine complex variety defined by the equation $q(x) = 0$; let \tilde{W} stand for the singular locus of an affine complex variety W . Finally, let $\Delta(f)$ be equal to the dimension of the affine complex variety defined by the condition $\text{rank } J(f) < r$, where

$$J(f) := \left(\frac{\partial f_j}{\partial x_i} \right), \quad 1 \leq j \leq r, \quad 1 \leq i \leq n,$$

stands for the Jacobian of the map

$$f : \mathbb{C}^n \rightarrow \mathbb{C}^m.$$

One can prove that $\Delta(f)$ is actually equal to the dimension of the Zariski closure of the union

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

of the loci of singularities of the affine varieties defined by the (systems of) equations

$$f(x) = \lambda, \quad \lambda \in \mathbb{C}^r,$$

if $\dim V(f) = n - r$, cf. [1].

Theorem 3. *Let $\vec{b} := (b_1, \dots, b_n)$ and let*

$$\mathfrak{B} = \prod_{j=1}^n [b_j - 1/2, b_j + 1/2).$$

(i) *If*

$$(7) \quad n > \Delta(f) + 2^{(d-1)} (d-1)r(r+1),$$

then the circle method works.

(ii) *Suppose that condition (7) is satisfied and $\dim V(f) = n - r$. Then*

$$\mu_\infty > 0$$

as soon as

$$(8) \quad \vec{b} \in (V(f) \setminus \tilde{V}(f))(\mathbb{R}),$$

and

$$\mu_0 > 0$$

as soon as

$$(9) \quad (V(f) \setminus V(\tilde{f}))(\mathbb{Z}_p) \neq \emptyset$$

for every p in \mathcal{P} .

(iii) In particular, if all the three conditions (7) – (9) are satisfied, then the circle method works well.

§4. Cubic Diophantine equations

In this section, we review rather old (but rarely cited) results of Dav-
enport, Lewis, and Watson. Suppose that $r = 1$, $d_1 = 3$ and write, for
brevity,

$$g := \vec{g}, \quad g = f + h,$$

where f is a cubic form and h is a quadratic polynomial. Following [3], [25],
[26], we let

$$\nu(g) = \min\{s \mid f = \sum_{i=1}^s l_i q_i\}$$

with linear l_i and quadratic q_i . Suppose the polynomial g be irreducible
and *non-degenerate*, that is not equivalent (over \mathbb{Z}) to a polynomial of less
than n variables. Suppose also the congruence

$$(10) \quad g(x) \equiv 0 \pmod{p^k}$$

be soluble for every prime power p^k , $p \in \mathcal{P}$. Then each of the following
three conditions implies solubility of the equation (2) in \mathbb{Z} :

(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 $q(x_1, \dots, x_{n-1})$
such that $f(x) = x_n q(x_1, \dots, x_{n-1})$, the quadratic form $q(x_1, \dots, x_{n-2}, 0)$
is positive definite, and equation (2) 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], [25], [26] for the detailed proof and a discussion
of the cited results.

Corollary 3. *If $n \geq 19$, $\nu(g) \geq 4$, and the congruence condition (10) is
satisfied, then equation (2) is soluble in \mathbb{Z} .*

These results allow one to isolate a big decidable subclass of cubic Dio-
phantine equations. One can hardly expect, however, the whole class of the
cubic equations be decidable.

The known results, concerning the 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 [7] that every *non-singular* form f represents zero non-trivially over \mathbb{Z} as soon as $n \geq 10$, and Hooley proved [10] 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 §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 quaternary 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 those problems (cf., for instance, [9]).

However, other methods of analytic number theory can sometimes be applied to study Diophantine equations having not too many solutions. For instance, as an application of A. Baker's estimates on linear forms in logarithms of algebraic integers, one can prove that the class of Thue and superelliptic equations is decidable (cf. [21]). The Birch and Swinnerton-Dyer conjecture, if true, can probably be used to prove \mathbb{Q} -decidability of the class of curves of genus one defined over \mathbb{Q} (cf., for instance, note 11.2, a) in [13] and [23, p. 160]); it would then follow that the class of the homogeneous cubic equations in three variables is decidable. Those problems lie far beyond the scope of this survey, however, and we shall not comment on these questions any further.

Acknowledgement. I am very much obliged to my colleagues and friends for their remarks and comments on some of the questions discussed in this

paper. A preliminary version of the note circulated as a Max-Planck-Institut für Mathematik Preprint, no. 118, 1999. This new version has been influenced by a few conversations with the participants of the Research Programme "Set Theory" at the CRM (Barcelona) in winter 2004. I use this opportunity to thank the Director and the staff of the CRM for their generous hospitality during my visit there.

REFERENCES

- [1] A.G.Aleksandrov and B.Z.Moroz, Complete intersections in relation to a paper of B.J.Birch, *Bulletin of the London Math. Soc.*, 34 (2002), 149-154.
- [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.
- [5] H.M. Friedman, Finite functions and the necessary use of large cardinals, *Annals of Mathematics*, 148 (1998), 803-893.
- [6] 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.
- [7] D.R. Heath-Brown, Cubic forms in ten variables, *Proc. of the London Math. Soc.*, 47 (1983), 225-257.
- [8] 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.
- [9] C. Hooley, Some recent advances in analytic number theory, *Proc. of the ICM 1983*, Warszawa, 85-97.
- [10] C. Hooley, On nonary cubic forms, *Journal für die reine und angew. Mathematik*, 386 (1988), 32-98.
- [11] T. Jech, *Set Theory*, Springer-Verlag, 2003.
- [12] L. Kirby and J. Paris, Accessible independence results for Peano Arithmetic, *Bulletin of the London Math. Soc.*, 14 (1982), 285-293.
- [13] Yu.I. Manin, Cyclotomic fields and modular curves, *Russian Mathematical Surveys*, 26 (1971), no. 6, 7-78.
- [14] Yu.V. Matiyasevich, Enumerable sets are Diophantine, *Doklady AN SSSR*, 191 (1970), 278-282 (translated in: *Soviet Math. Doklady*, 11 (1970), 354-358).
- [15] Yu.V. Matiyasevich, Hilbert's tenth problem: What was done and what is to be done, in: *Hilbert's tenth problem: Relations with arithmetic and algebraic geometry* (J. Denef et al., eds.), *Contemporary Mathematics*, 270 (2000), 1-47.
- [16] Yu.V. Matiyasevich, *Hilbert's Tenth Problem*, The MIT Press, 1993.
- [17] J. Robinson, Solving Diophantine equations, *Proceedings of the 4th International Congress for Logic, Methodology, and Philosophy of Science* (P.C. Suppes et al., eds.), North-Holland, Amsterdam, 63-67 (*Collected Works*, S. Feferman, ed., AMS, 1996, 205-209).
- [18] W.M. Schmidt, The density of integer points on homogeneous varieties, *Acta Math.*, 154 (1985), 243-296.

- [19] A. Shlapentokh, On Diophantine definability and decidability in some infinite totally real extensions of \mathbb{Q} , *Transactions of the American Math. Soc.*, 356 (2004), 3189-3209.
- [20] J.R. Shoenfield, *Mathematical Logic*, Addison-Wesley publishing Company, 1967.
- [21] T.D. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Maths no. 87, Cambridge Univ. Press, 1986.
- [22] C.M. Skinner, Forms over number fields and weak approximation, *Compositio Math.*, 106 (1997), 11-29.
- [23] Sir Peter Swinnerton-Dyer, Diophantine equations: the geometric approach, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 98 (1996), 146-164.
- [24] R.C. Vaughan, *The Hardy-Littlewood circle method*, Cambridge Tracts in Maths, 125, Cambridge Univ. Press, 1997.
- [25] G.L. Watson, Non-homogeneous cubic equations, *Proc. of the London Math. Soc.*, 17 (1967), 271-295.
- [26] G.L. Watson, Cubic Diophantine equations with reducible cubic part, *Proc. of the London Math. Soc.*, 21 (1970), 181-200.
- [27] T.D. Wooley, An explicit version of Birch's theorem, *Acta Arithmetica*, 85 (1998), 79-96.
- [28] 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.

B.Z. MOROZ: MAX-PLANCK-INSTITUT FÜR MATHEMATIK,
VIVATSGASSE 7, D-53111 BONN, GERMANY
E-mail address: moroz@mpim-bonn.mpg.de