Undecidable and decidable restrictions of Hilbert's Tenth Problem: images of polynomials *vs.* images of exponential functions

Mihai Prunescu *

Abstract

Classical results of additive number theory lead to the undecidability of the existence of solutions for diophantine equations in given special sets of integers. Those sets which are images of polynomials are covered by a more general result in the second section. In contrast, restricting diophantine equations to images of exponential functions with natural bases leads to decidable problems, as proved in the third section.
A.M.S. Classification: 03D40.

1 Introduction

We start by recalling some facts about Hilbert's Tenth Problem and its restrictions. Let R be a commutative ring with 1 and let $A \subseteq R$ any subset. We denote the ring $\mathbb{Z}[X_1, X_2, \ldots, X_n, \ldots]$ in countably many variables by $\mathbb{Z}[\omega]$.

Definition: Hilbert's Tenth Problem restricted to the set A is the set:

$$\text{HTP } [A] := \{P \in \mathbb{Z}[\omega] \mid \exists n \in \mathbb{N}\ \exists \vec{x} \in A^n \quad P(\vec{x}) = 0\}.$$

For all rings R and subsets A one can put the question of the decidability of the set HTP $[A]$. Hilbert's Tenth Problem in its original form was if HTP $[\mathbb{N}]$ is decidable. This has been answered negatively by Matiyasevich, see [8], the same for HTP $[\mathbb{Z}]$.

A lot of work has been put in proving that equations with coefficients in $\mathfrak{O}_K$ are undecidable for rings of algebraic integers $\mathfrak{O}_K$ in number fields K (finite extensions of the field of rational numbers $\mathbb{Q}$), but only some cases have been proved so far, see [2], [3], [4], [11], [15], [16]. All these results have been achieved by constructing diophantine definitions with coefficients in $\mathfrak{O}_K$ for the ring of integers $\mathbb{Z}$ in $\mathfrak{O}_K$. But it is easy to prove that if $\mathbb{Z}$ has a diophantine definition in $\mathfrak{O}_K$ with coefficients in $\mathfrak{O}_K$, then it has also a diophantine definition in $\mathfrak{O}_K$ with coefficients in $\mathbb{Z}$. Further one has to relativize all unknowns occuring in polynomials in $\mathbb{Z}[\omega]$ to this definition and to repeatedly use a special polynomial $p \in \mathbb{Z}[x, y]$ (in $\mathfrak{O}_K$ holds that $p(x, y) = 0$ is equivalent with $x = y = 0$), in order to transform systems of equations in individual equations. So we have many examples of number fields K such that HTP $[\mathfrak{O}_K]$ is undecidable, but we do not know this in general.

The problem about the decidability of HTP $[\mathbb{Q}]$ is also open and very difficult.

In this paper we will consider problems of the form HTP $[A]$ for some special subsets A of the ring $\mathbb{Z}$ of the integers. In order to motivate our work we display a general principle permitting us to apply results of the additive number theory for cases of HTP $[A]$. Start with a short Remark:

*Universität Freiburg, Germany; and IMAR Bucharest, Romania. This research was supported by the DFG over a post-doctoral grant in the *Graduiertenkolleg Mathematische Logik und Anwendungen*.

Remark 1.1 *Hilbert's Tenth Problem restricted to ideals in $\mathbb{Z}$ and to arithmetic progressions, that is* HTP $[k\mathbb{Z}]$ *and* HTP $[a+k\mathbb{N}]$ *(with $k \neq 0$), are undecidable.*

Proof:

$$\exists\, \vec{x} \in \mathbb{Z} \quad P(\vec{x}) = 0 \quad \Leftrightarrow \bigvee_{\vec{\imath} \in \{0,\ldots,k-1\}^m} \exists\, \vec{y} \in k\mathbb{Z} \quad P(\vec{y} + \vec{\imath}) = 0.$$

So deciding the solvability of an equation with m unknowns over $\mathbb{Z}$ is equivalent to deciding the solvability of k^m many equations over the ideal $k\mathbb{Z}$. If HTP $[k\mathbb{Z}]$ was decidable, one could decide if the equation $P(\vec{x}) = 0$ has solutions in $\mathbb{Z}$ by repeating the decision algorithm for HTP $[k\mathbb{Z}]$ for k^m times. Contradiction.

For the arithmetic progressions we observe that:

$$\exists\, \vec{y} \in k\mathbb{Z} \quad P(\vec{y}) = 0 \quad \Leftrightarrow \quad \exists\, \vec{u}, \vec{v} \in a + k\mathbb{N} \quad P(\vec{u} - \vec{v}) = 0.$$

□

We observe that for all $k \in \mathbb{N} \setminus \{0\}$, the set $k\mathbb{N} \cup \{0, 1\}$ is an additive basis of order k for $\mathbb{N}$.

Definition: Let B be a set such that $\{0,1\} \subset B \subset \mathbb{N}$. B is called additive basis of order $k \geq 1$ for the set $\mathbb{N}$ if $\forall\, n \in \mathbb{N}\ \exists\, x_1, \ldots, x_k \in B \quad n = x_1 + \cdots + x_k$. Similarly we define additive bases for $\mathbb{Z}$ or for arbitrary rings.

Definition: For some $A \subset \mathbb{Z}$ and $s \in \mathbb{Z}$ we denote by $A_{\geq s}$ the set $\{x \in A \,|\, x \geq s\}$. With the similar meaning we use $A_{<s}$.

Remark 1.2 *Let $A \subset \mathbb{N}$ and $k \geq 1$ be such that $A \cup \{0,1\}$ is an additive basis of order k for $\mathbb{N}$. Then all the problems* HTP $[A_{\geq s}]$ *are undecidable.*

Proof: The set $A_{<s}$ is some finite set of natural numbers, say $\{a_1, a_2, \ldots, a_n\}$. One has the equivalence:

$$\exists\, \vec{x} \in \mathbb{N} \quad P(\vec{x}) = 0 \quad \Leftrightarrow \bigvee_{y_i^j \in \{0,1\} \cup A_{<s} \cup \{z_l\}} \exists\, \vec{z} \in A_{\geq s} \quad P\,(\sum_{j=1}^{k} y_1^j, \ldots, \sum_{j=1}^{k} y_m^j) = 0.$$

Here z_l are new variables, and every old unknown x_i is substituted by a sum $\sum_{j=1}^{k} y_i^j$ of constants in $\{0,1\} \cup A_{<s}$ or new unknowns z_l. Hence, deciding the solvability of some equation with m unknowns in $\mathbb{N}$ reduces to get the answer for $\leq (n+3)^{mk}$ equations in $A_{\geq s}$. If this second task would be decidable, then the existence of solutions in $\mathbb{N}$ would have been decidable too. □

Definition: For $m \geq 3$ and $k, l \in \mathbb{N}$ we denote the number $(1/2)(m-2)k(k-1)+k$ by $p_m(k)$ and call it the k-th. m-polygonal number. For $m = 3, 4, 5$ this gives the popular triangular numbers, squares, penthagonal numbers, respectively.

Corollary 1.3 *The following problems* HTP $[A]$, HTP $[A_{\geq s}]$ *are undecidable:*

- $A \subseteq \mathbb{N}$ *with Schnirelmann density $\delta(A) > 0$.*
- $A = p_m(\mathbb{N})$, *the set of m-polygonal numbers for $m \geq 3$.*
- $A = (\mathbb{N})^g := \{n^g \,|\, n \in \mathbb{N}\}$, *the set of g-th. powers of natural numbers.*
- $A = \mathfrak{P}$, *the set of natural prime numbers.*

Proof: Generally, if $\{0,1\} \subset A \subseteq \mathbb{N}$ with $\delta(A) > 0$ then A is an additive basis of $\mathbb{N}$, see [14], [9] or [7]. For example, an arithmetic progression extended with the elements 0 and 1 is a set with positive density. Also, if we denote by $\mathcal{A}$ the set of square-free natural numbers then $\delta(\mathcal{A}) = 53/88$ as proven in [12]. The other examples in 1.3 are sets with zero density.

It has been conjectured by Fermat that the sets $p_m(\mathbb{N})$ are additive bases for the naturals. After partial solutions by Lagrange and Gauss, this has been proved by Cauchy, [1].

The conjecture that the sets $\mathbb{N}^g$ are additive bases for the naturals was known as Waring's Problem. This was proved by Hilbert in 1908, see [5].

According to Schnirelmann, the set $\mathfrak{P} \cup \{0,1\}$ is an additive basis of $\mathbb{N}$ and we apply the Remark 1.2. See [14], [18] or [9]. Alternatively, according to Vinogradov [18] sufficiently large natural numbers are sums of three primes, so arbitrary integers are sum and difference of six primes.

All proofs can be also found in the monograph [9]. □

With these results we exhausted the possibilities given by the classical additive number theory together with the Remark 1.2. Our goal in this paper is to generalize those results in 1.1 and 1.3 concerning images of polynomial functions and to give a shorter, self-contained proof for this generalization.

2 Images of polynomials

Because of the m-polygonal numbers in 1.3, for generalizing 1.1 and 1.3 it is not sufficient to restrict ourselves to images of polynomials with coefficients in $\mathbb{Z}$.

Definition: We denote by $\mathfrak{R}$ the ring of those polynomials $f \in \mathbb{Q}[t]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$. $\mathfrak{R}$ is called the ring of integral-valued polynomials.

Definition: By an infinite interval of integers we understand an element I of the set

$$\{\mathbb{Z}\} \cup \{a + \mathbb{N} \,|\, a \in \mathbb{Z}\} \cup \{a - \mathbb{N} \,|\, a \in \mathbb{Z}\}.$$

We observe that HTP $[f(I)]$ corresponds also to a syntactical restriction of Hilbert's Tenth Problem. It is asked about the existence of solutions in I for equations $P(\vec{x}) = 0$ with polynomials $P \in \mathbb{Z}[f(X_1), f(X_2), \ldots, f(X_n), \ldots]$.

Theorem 2.1 *Let $f \in \mathfrak{R} \setminus \mathbb{Z}$ be a non-constant polynomial and let $I \subseteq \mathbb{Z}$ be an infinite interval of integers. Then the restricted Hilbert's Tenth Problem* HTP $[f(I)]$ *is undecidable.*

For the proof, a small machinery based on polynomial identities shall be developed. The following Lemma is an algebraic identity given by Tardy in 1851, see [17]. This identity has been used by Sierpinski to prove that for all powers n, the set $(\mathbb{Z})^n \cup -(\mathbb{Z})^n$ is an additive basis for $\mathbb{Z}$, see [13], page 399.

Lemma 2.2 *The following identity holds:*

$$\sum_{\vec{\sigma} \in \{0,1\}^n} \left(-1\right)^{\sum_{i=1}^{n} \sigma_i} \left(\sum_{i=1}^{n} (-1)^{\sigma_i} x_i\right)^n = 2^n \cdot n! \cdot x_1 x_2 \ldots x_n.$$

Proof: Consider some monomial $\vec{x}^{\vec{\alpha}}$ different from $x_1 x_2 \ldots x_n$ occurring in the development of the left hand side. At least one variable x_i, say x_n, is missing, so $\alpha_n = 0$. One gets:

$$c_{\vec{\alpha}} \vec{x}^{\vec{\alpha}} \left(\sum_{\vec{\sigma} \in \{0,1\}^n} \left(-1\right)^{\sum_{i=1}^{n} \sigma_i} \left(-1\right)^{\sum_{i=1}^{n} \alpha_i \sigma_i} \right) = c_{\vec{\alpha}} \vec{x}^{\vec{\alpha}} \left(\sum_{\vec{\sigma} \in \{0,1\}^n} \left(-1\right)^{\sum_{i=1}^{n} (\alpha_i + 1) \sigma_i} \right) =$$

$$= c_{\vec{\alpha}}\vec{x}^{\vec{\alpha}}\left(\sum_{\vec{\sigma}\in\{0,1\}^{n-1}\times\{0\}}\left(-1\right)^{\sum_{i=1}^{n-1}(\alpha_i+1)\sigma_i} - \sum_{\vec{\sigma}\in\{0,1\}^{n-1}\times\{1\}}\left(-1\right)^{\sum_{i=1}^{n-1}(\alpha_i+1)\sigma_i}\right) = 0.$$

For the monomial $x_1x_2\ldots x_n$ we get $c_{\vec{\alpha}} = n!$ and the sign $(-1)^{(2\sum\sigma_i)} = 1$ exactly 2^n times. □

Lemma 2.3 *For all numbers k with $0 \leq k < n$ the following identity holds:*

$$\sum_{\vec{\sigma}\in\{0,1\}^n}\left(-1\right)^{\sum_{i=1}^{n}\sigma_i}\left(\sum_{i=1}^{n}(-1)^{\sigma_i}x_i\right)^k = 0.$$

Proof: In every occurring monomial is at least one missing variable because $k < n$. We proceed like in the precedent proof. □

Lemma 2.4 *Let $f = a_nt^n + \cdots + a_1t + a_0$ be a polynomial with $a_n \neq 0$. Then the following identity holds:*

$$\sum_{\vec{\sigma}\in\{0,1\}^n}\left(-1\right)^{\sum_{i=1}^{n}\sigma_i} \cdot f\left(\sum_{i=1}^{n}(-1)^{\sigma_i}x_i\right) = 2^n\cdot n!\cdot a_n\cdot x_1x_2\ldots x_n.$$

Proof: According to Lemma 2.2 the leading coefficient has the given contribution in the sum. According to Lemma 2.3 the other coefficients have not any contribution. □

Lemma 2.5 *Let $f \in \Re\setminus\mathbb{Z}$ be some polynomial. Then the set*

$$f(\mathbb{Z})\cup -f(\mathbb{Z})\cup\{0,1\}$$

is an additive basis of finite order for the ring $\mathbb{Z}$.

Proof: In Lemma 2.4 set $x_1 = x_2 = \cdots = x_n = 1$. We get that $v := 2^n\cdot n!\cdot a_n \in \mathbb{Z}\setminus\{0\}$. Now take $x_1 = x_2 = \cdots = x_{n-1} = 1$ and $x_n = x \in \mathbb{Z}$ arbitrary. It follows that all elements in the ideal $v\mathbb{Z}$ are sums of 2^n many elements of the set $f(\mathbb{Z})\cup -f(\mathbb{Z})$. But this means that all elements in $\mathbb{Z}$ are sums of $2^n + |v|$ many elements of the set $f(\mathbb{Z})\cup -f(\mathbb{Z})\cup\{0,1\}$. □

Lemma 2.6 *Let $f \in \Re\setminus\mathbb{Z}$ be some polynomial and $I \subseteq \mathbb{Z}$ be an infinite interval of integers. Then the set*

$$f(I)\cup -f(I)\cup\{0,1\}$$

is an additive basis of finite order for the ring $\mathbb{Z}$.

Proof: For the case $I = \mathbb{Z}$ we have just shown it. By substituting $f(t) \in \Re$ with $f(t-a) \in \Re$, it is enough to consider the cases $I = \mathbb{N}$ and $I = -\mathbb{N}$. If $I = \mathbb{N}$ then let $h(t) := f(t^2) \in \Re$. Then $h(\mathbb{Z}) \subseteq f(\mathbb{N})$, so also

$$h(\mathbb{Z})\cup -h(\mathbb{Z})\cup\{0,1\} \subseteq f(\mathbb{N})\cup -f(\mathbb{N})\cup\{0,1\},$$

and a superset of an additive basis of a ring is an additive basis of at most the same order for this ring. If $I = -\mathbb{N}$ then take $h(t) := f(-t^2) \in \Re$ and repeat the argument with $h(\mathbb{Z}) \subseteq f(-\mathbb{N})$. □

Proof of the theorem 2.1: Let $P(\vec{x}) = 0$ an equation with m unknowns and let $k = 2^n + |v|$ be the order of the additive basis $f(I)\cup -f(I)\cup\{0,1\}$ for $\mathbb{Z}$. It holds that:

$$\exists\,\vec{x}\in\mathbb{Z}\quad P(\vec{x}) = 0 \quad\Leftrightarrow \bigvee_{y_i^j\in\{0,1\}\cup\{z_l\}\cup\{-z_l\}} \exists\,\vec{z}\in f(I)\quad P\left(\sum_{j=1}^{k}y_1^j,\ldots,\sum_{j=1}^{k}y_m^j\right) = 0.$$

So arbitrary equations over $\mathbb{Z}$ are equivalent with disjunctions of $\leq 4^{mk}$ many equations over $f(I)$. If HTP $[f(I)]$ would have been decidable, so was also HTP $[\mathbb{Z}]$. Contradiction. □

Corollary 2.7 *Let be $f \in \mathfrak{R}$ a non-constant polynomial. It is undecidable if arbitrary diophantine equations $P(\vec{x}) = 0$ with polynomials $P \in \mathbb{Z}[f(X_1), f(X_2), \ldots, f(X_n), \ldots]$ have solutions in $\mathbb{Z}$ or in some infinite interval of integers I.*

Remark 2.8 *All these results generalize trivially to polynomials in more than one variable, because the image of such a non-constant polynomial contains the image of a non-constant polynomial in one variable.*

Another syntactic restriction of Hilbert's Tenth Problem can be defined: HTPS $[A]$, Hilbert's Tenth Problem over A for symmetric polynomials:

$$\text{HTPS } [A] := \{P \in \mathbb{Z}[\omega] \mid P \text{ symmetric and } \exists n \in \mathbb{N}\ \exists \vec{x} \in A^n \quad P(\vec{x}) = 0\,\}.$$

For some polynomial $P \in \mathbb{Z}[X_1, \ldots, X_n]$ let the polynomial SP be defined by:

$$SP(\vec{X}) := \prod_{\sigma \in S_n} P(\sigma(\vec{X})),$$

where $\sigma(\vec{X}) := (X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. If the ring R is a domain and $A \subseteq R$ then it holds:

$$\exists \vec{x} \in A^n \quad P(\vec{x}) = 0 \iff \exists \vec{x} \in A^n \quad SP(\vec{x}) = 0.$$

Remark 2.9 *For all integral domains R and subsets $A \subseteq R$, the problem* HTP $[A]$ *is undecidable if and only if the problem* HTPS $[A]$ *is undecidable.*

3 Images of exponential functions

One should not believe that any restriction of HTP to some infinite recursive subset of $\mathbb{N}$ is undecidable. We are going to see some decidable restrictions of Hilbert's Tenth Problem, in contrast with the results in Section 2.

Definition: Let $k \in \mathbb{N}$ be a number with $k \geq 2$. We denote by $k^{\mathbb{N}}$ the set $\{k^n \mid n \in \mathbb{N}\}$.

We observe that HTP $[k^{\mathbb{N}}]$ corresponds also to a syntactical restriction of Hilbert's Tenth Problem, because the recursive set $k^{\mathbb{N}}$ has a diophantine definition in $\mathbb{Z}$.

Theorem 3.1 *The problems* HTP $[k^{\mathbb{N}}]$ *and* HTP $[k^{\mathbb{N}}{}_{>s}]$ *are decidable.*

First proof: The theorem follows directly from the result proved by van den Dries in [6]. He proved there that the structure $(\mathbb{R}, +, -, \cdot, \leq, A(\,\cdot\,))$ (with an unary predicate $A(\,\cdot\,)$ to be satisfied only by the elements of $k^{\mathbb{Z}}$) is decidable. It is immediate to see that the fact that some diophantine equation has a solution in $k^{\mathbb{N}}$ is equivalent with a formal statement over this structure. □

Van den Dries proved that the theory $\mathcal{RCF}$ of real closed fields together with the axioms: A is a multiplicative subgroup consisting of positive elements, $A(k)$, $\forall\, x\ (1 < x < k \to \neg A(x))$ and $\forall\, x\ (x > 0 \to \exists\, y\ A(y) \wedge y \leq x < ky)$ is a complete theory with a recursive axiomatization, hence decidable. His proof doesn't give any concrete decision procedure.

Second proof: This is a sketch of the decision procedure. Write the equation $P(\vec{x}) = 0$ in the form $Q(\vec{x}) = R(\vec{x})$ where $Q, R \in \mathbb{N}[\vec{x}]$. Write all the coefficients according to the k-ary system (in the basis $k \geq 2$) and put $x_i = k^{y_i}$. According to the k-ary representation system every monomial $c_{\vec{\alpha}}\vec{x}^{\vec{\alpha}}$ looks like $\overline{w}00\ldots0$, where $\overline{w}$ is a word in the alphabet $\{\underline{0}, \underline{1}, \ldots, \underline{k-1}\}$ concatenated with a word consisting of $\sum \alpha_i y_i$ many zeros. Because the only nontrivial information comes from the k-ary representation of the coefficients and from the number of zeros, there are only finitely many cases to check in order to decide if the equality is possible. □

Corollary 3.2 (to the second proof). *The followig set is also decidable:*

$$\bigcup_{k\in\mathbb{N}} \mathrm{HTP}[k^{\mathbb{N}}].$$

Remark 3.3 *With the same methods we can prove that the problems* HTP $[f(k^{g(\mathbb{N})})]$ *are decidable for all* $f, g \in \mathfrak{R}$.

There are some other problems of interest with analytic superexponential functions:

Open questions: *What can be said about the decidability of* HTP $[f(\mathbb{N})]$ *for (i)* $f(n) = n!$ *and (ii)* $f(n) = n^n$ *?*

In [13] (pg. 108 - 109) Sierpinski gives infinite families of solutions for the equation $XY = Z$ considered in both contexts.

According to Nathanson's results in [10] for all function $f : \mathbb{R} \to \mathbb{R}$ with $\lim_{x\to\infty} f(x) = \infty$ there are (recursive) additive bases of order 2 for the integers such that the number of basis elements between $-x$ and x is bounded by $f(x)$. Since the corresponding HTP's are undecidable, we see that this decidability question is not really a problem of increment-rate.

Acknowledgment: The author thanks Karin Halupczok for some conversations concerning the classical additive number theory.

References

[1] **Augustin Louis Cauchy**: *Démonstration du théorème général de Fermat sur les nombres polygones.* Mem. Sci. Math. Phys. Inst. France, 14 (1), 177 - 220, 1813.

[2] **Jan Denef**: *Hilbert Tenth Problem for quadratic rings.* Proceedings of the American Mathematical Society, 48 (1), 214 - 220, 1975.

[3] **Jan Denef**: *Diophantine sets over algebraic integer rings II.* Transactions of the American Mathematical Society, 257 (1), 227 - 236, 1980.

[4] **Jan Denef, Leonard Lipshitz**: *Diophantine sets over some rings of algebraic integers.* Journal of the London Mathematical Society (Second Series), 18 (3), 385 - 391, 1978.

[5] **David Hilbert**: *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl* n^{ter} *Potenzen (Waringsches Problem).* Mathematische Annalen, 67, 281 - 300, 1909.

[6] **Lou van den Dries**: *The field of reals with a predicate for the powers of two.* Manuscripta Mathematica 54, 187 - 195, 1985.

[7] **Aleksandr Yakovlevich Khinchin**: *Three pearls of number theory.* New edition: Dover 1998, after a copyright from 1952.

[8] **Yuri Matiyasevich**: *Hilbert's Tenth Problem.* The MIT Press, London, 1993.

[9] **Melvyn Nathanson**: *Additive Number Theory - The Classical Bases* -. Springer Verlag, Graduate Texts in Mathematics, 1997.

[10] **Melvyn Nathanson**: *Unique representation bases for the integers.* arXiv:math.NT/0202137v1, 2002.

[11] **Thanases Pheidas**: *Hilbert's Tenth Problem for a class of rings of algebraic integers.* Proceedings of the American Mathematical Society, 104 (2), 611 - 620, 1988.

[12] **Kenneth Rogers**: *The Schnirelmann density of squarefree integers.* Proceedings of the A.M.S. 15, 515 - 516, 1964.

[13] **Waclaw Sierpinski**: *Elementary Theory of Numbers.* Polska Akademia Nauk Monografie Matematyczne, Warszawa 1964.

[14] **Lev Genrikhovich Schnirelmann**: *Über additive Eigenschaften von Zahlen.* Mathematische Annalen, 107, 649 - 690, 1933.

[15] **Harold Shapiro, Alexandra Shlapentokh**: *Diophantine relationship between algebraic number fields.* Communications on Pure and Applied Mathematics 42 (8), 1113 - 1122, 1989.

[16] **Alexandra Shlapentokh**: *Extensions of Hilbert's Tenth Problem to some algebraic number fields.* Communications on pure and Applied Mathematics 43 (8), 1055 - 1066, 1990.

[17] **Placido Tardy**: *Transformazione di un prodotto di n fattori.* Ann. Sc. Mat. e. Fis. 2, 287 - 291, 1851.

[18] **Ivan Matveevich Vinogradov**: *Representation of an odd number as the sum of three primes.* Doklady Akad. Nauk SSSR, 15 (6 - 7), 291 - 294, 1937. English translation in *Selected Works*, 101 - 106, Springer Verlag, 1985.