Yu. V. Matiyasevich, The existence of non-effectivizable estimates in the theory of exponential Diophantine equations, *Zap. Nauchn. Sem. LOMI*, 1974, Volume 40, 77–93

Ю.В.Матиясевич

СУЩЕСТВОВАНИЕ НЕЭФФЕКТИВИЗИРУЕМЫХ ОЦЕНОК В ТЕОРИИ ЭКСПОНЕНЦИАЛЬНО ДИОФАНТОВЫХ УРАВНЕНИЙ

(Основные результаты доложены 31 мая 1973г.)

I. Введение. Пусть

$$\mathcal{D}(x_1, \ldots, x_\alpha) = 0$$

– некоторое диофантово уравнение, про которое доказано, что оно имеет разве лишь конечное число решений в целых числах. Доказательство ограниченности числа решений может нести разную информацию о самих решениях. В некоторых случаях из доказательства можно извлечь верхнюю оценку для абсолютных величин неизвестных, то есть такое число c, что для любого решения рассматриваемого уравнения $\max\{|x_1|, \ldots, |x_\alpha|\} \leq c$. Ясно, что в таком случае мы можем эффективно найти и сами решения.

С другой стороны, доказательство ограниченности числа решений может быть проведено методом reductio ad absordum. В таком случае верхняя оценка не может не существовать, но мы не будем иметь способа ни для ее вычисления, ни для нахождения самих решений; в этой ситуации говорят, что оценка неизвестных неэффективна. Классическим примером здесь может служить теорема А.Туэ [I] о том, что если F – неприводимая бинарная форма не менее, чем 3-ей степени, то однородное диофантово уравнение

$$F(x, y) = a$$

при каждом значении параметра a имеет разве лишь конечное число решений. Исходным пунктом доказательства Туэ являлось предположение о том, что рассматриваемое уравнение имеет сколь угодно большие решения (точнее, что оно имеет достаточно большое решение в некотором специальном смысле). Это обстоятельство и не позволяет извлечь из доказательства Туэ эффективно вычислимую оценку.

Несмотря на усилия многих математиков, в течение долгого времени никому не удавалось усилить результат Туэ до получения эффективно вычислимой оценки неизвестных. Это сделал лишь сравнительно недавно А.Бейкер [2], опираясь на свои глубокие результаты об оценке линейных форм от логарифмов алгебраических чисел. Цель настоящей статьи – показать, что трудности, стоящие на пути перехода от неэффективных оценок к эффективно вычислимым, могут, вообще говоря, быть и принципиального характера, а не только технического. А именно, будет показано, что если рассматривать более широкий класс уравнений (конкретно, класс экспоненциально диофантовых урав-

нений), то не все результаты об ограниченности числа решений, полученные неэффективными способами, будут допускать эффективизацию. Примеры неэффективизируемых результатов дают приводимые ниже два следствия из основной теоремы настоящей работы.

СЛЕДСТВИЕ I. Можно указать конкретный полином $A(a, x_1, \ldots, x_\nu)$ с целочисленными коэффициентами, который обладает следующими двумя свойствами. Во-первых, для любого натурального значения параметра a уравнение

$$A(a, x_1, \ldots, x_\nu) = y + 4^y \qquad (I)$$

имеет не более одного решения в натуральных $x_1, \ldots, x_\nu, y$ и, следовательно, для каждого a не может не существовать такое число c, что для любых $x_1, \ldots, x_\nu, y$ удовлетворяющих (I), справедливо неравенство

$$\max\{x_1, \ldots, x_\nu, y\} \leq c.$$

Во-вторых, какова бы ни была одноместная общерекурсивная (то есть определенная на всех натуральных числах эффективно вычислимая натуральнозначная) функция C, можно найти натуральные числа $a, x_1, \ldots, x_\nu, y$, удовлетворяющие (I) и неравенству

$$\max\{x_1, \ldots, x_\nu, y\} > C(a).$$

СЛЕДСТВИЕ 2. Можно указать конкретный полином $B(a, x_0, \ldots, x_{\varkappa}, y, z)$ с целочисленными коэффициентами, который обладает следующими двумя свойствами. Во-первых, при любом натуральном значении параметра a неравенство

$$B(a, x_0, \ldots, x_{\varkappa}, y, 2^y) > 0 \qquad (2)$$

имеет место не более, чем при одном наборе значений $x_0, \ldots, x_{\varkappa}, y$ и, следовательно, для каждого a не может не существовать такое число c, что для любых $x_0, \ldots, x_{\varkappa}, y$ справедливо неравенство

$$B(a, x_0, \ldots, x_{\varkappa}, y, 2^y) \leq c.$$

Во-вторых, для любой одноместной общерекурсивной функции C можно найти натуральные числа $a, x_0, \ldots, x_{\varkappa}, y$ такие, что

$$B(a, x_0, \ldots, x_{\varkappa}, y, 2^y) > C(a). \qquad (3)$$

Интересно было бы получить аналогичные результаты для диофантовых уравнений и неравенств. Теорема о диофантовости перечислимых предикатов (см., например, [3] - [5]) позволяет легко получить следующий результат: можно указать полином $B^*(a, x_0, \ldots, x_\lambda)$ такой, что, с одной стороны, при любом натуральном значении параметра a уравнение

$$B^*(a, x_0, \ldots, x_\lambda) = c$$

разрешимо не более, чем при одном значении параметра c, а с другой стороны, для любой одноместной общерекурсивной функции C можно найти числа $a, x_0, \ldots, x_\lambda$ такие, что

$$B^*(a, x_0, \ldots, x_\lambda) > C(a).$$

Этот результат не сильнее следствия 2, поскольку здесь не предполагается единственность $x_0, \ldots, x_\lambda$.

Чтобы получить для диофантовых уравнений результаты, аналогичные следствиям I и 2, было бы достаточно показать, что каждый перечислимый предикат имеет однократное диофантово представление (определение однократного представления см. ниже), а для этого, в свою очередь, было бы достаточно, согласно результатам данной работы, показать, что однократное диофантово представление имеет предикат $z = 2^y$. К сожалению, ни одно из опубликованных диофантовых представлений предиката $a = b^c$ (см. [3] - [9]) не является однократным. В связи с этим представляет интерес гипотеза М.Дейвиса о том, что уравнение

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2$$

не имеет решений за исключением тривиального $u = r = 1$, $v = s = 0$. В [10] показано, что из справедливости этой гипотезы следует существование диофантова представления предиката $a = b^c$. Гипотеза Дейвиса в ее первоначальной форме была опровергнута в [11] , однако в действительности вместо предположения об отсутствии нетривиальных решений достаточно более слабой гипотезы о конечности числа решений (см. [4]). Более того, несложный анализ показывает, что уже из этой слабой формы гипотезы следует существование даже однократного диофантова представления предиката $a = b^c$. В связи с гипотезой Дэйвиса Г.В.Чудновский в [7] объявил, что исследуя арифметические свойства последовательности решений уравнения $9x^2 - 7y^2 = 2$ можно получить явное диофантово представление предиката $y = 2^x \,\&\, x > C$, где C - некоторая константа. Отсутствие доказательства в [7] не позволяет ответить на вопрос, является ли получающееся представление однократным.

2. Формулировка основной теоремы. Всюду ниже строчные латинские буквы используются в качестве переменных для натуральных, то есть целых неотрицательных чисел; под полиномами понимаются полиномы с целочисленными коэффициентами, если не оговорено противное.

Будем говорить, что формула вида $(\exists z_1 \dots z_k)\mathcal{R}$ где $\mathcal{R}$ – формула с параметрами $a_1, \dots, a_l$, $z_1, \dots, z_k$ однократно представляет предикат $\mathcal{P}(a_1, \dots, a_l)$, если

$$(\exists z_1, \dots, z_k) \Longrightarrow (a_1, \dots, a_l)$$

и

$$\mathcal{P}(a_1, \dots, a_l) \Longrightarrow (\exists! z_1, \dots, z_k)$$

(или, что то же самое, если

$$\mathcal{P}(a_1, \dots, a_l) \Longleftrightarrow (\exists z_1 \dots z_k)$$

и

$$\mathcal{P}(a_1, \dots, a_l) \Longleftrightarrow (\exists! z_1 \dots z_k)\ ).$$

ОСНОВНАЯ ТЕОРЕМА. Каждый перечислимый предикат $\mathcal{P}(a_1, \dots, a_l)$ однократно представим некоторой формулой вида

$$(\exists z_1 \dots z_k)[\mathcal{A} = \mathcal{B}],$$

где $\mathcal{A}$ и $\mathcal{B}$ – выражения, построенные из натуральных чисел и переменных $a_1, \dots, a_l$, $z_1, \dots, z_k$ с помощью сложения, умножения и возведения в степень.

Эта теорема является усилением основного результата работы М.Дейвиса, Х.Патнама и Дж.Робинсон [I2] (полное изложение этого результата вместе с необходимыми сведениями из теории алгорифмов дано также в [I3]). Приводимое ниже доказательство является, по-существу, модификацией доказательства из [I2] . Основной причиной, приводящей к неоднократности представлений из [I2] , является китайская теорема об остатках, используемая дважды: при получении арифметического представления с одним квантором общности (теорема Дейвиса [I4]) и при переходе от этого представления к экзистенциальному. Воспользовавшись теоремой о диофантовости перечислимых предикатов (см., например, [3] – [5]), мы получим необходимое усиление теоремы Дейвиса без использования китайской теоремы об остатках, а применение усиленной формы этой теоремы даст возможность построить однократное экспоненциально диофантово представление. Остальные отличия от [I2] не связаны с необходимостью получить именно однократное представление.

3. Доказательство основной теоремы. Для упрощения записи ограничимся в доказательствах рассмотрением случая одноместного предиката – легко проследить, что все рассуждения проходят и для случая предикатов произвольной местности. Сформулируем предварительно ряд вспомогательных утверждений.

3.I. Если формула

$$(\exists z_1 \dots z_\varkappa) Q(a_1, \dots, a_\lambda, z_1, \dots, z_\varkappa)$$

однократно представляет предикат $\mathcal{P}(a_1, \dots, a_\lambda)$, а формула

$$(\exists y_1 \dots y_\nu) \mathcal{R}(a_1, \dots, a_\lambda, z_1, \dots, z_\varkappa, y_1, \dots, y_\lambda)$$

однократно представляет предикат $Q(a_1, \dots, a_\lambda, z_1, \dots, z_\lambda)$, то формула

$$(\exists z_1 \dots z_\varkappa\ y_1 \dots y_\nu) \mathcal{R}(a_1, \dots, a_\lambda, z_1, \dots, z_\varkappa, y_1, \dots, y_\nu)$$

однократно представляет предикат $\mathcal{P}(a_1, \dots, a_\lambda)$.

3.2. Если формулы $(\exists z_1 \dots z_\varkappa)[S = 0]$ и $(\exists y_1 \dots y_\nu)[T = 0]$ однократно представляют предикаты $\mathcal{P}(a_1, \dots, a_\lambda)$ и $Q(b_1, \dots, b_\mu)$ соответственно, то формула

$$(\exists z_1 \dots z_\varkappa\ y_1 \dots y_\nu)[S^2 + T^2 = 0]$$

однократно представляет предикат

$$\mathcal{P}(a_1, \dots, a_\lambda) \& Q(b_1, \dots, b_\mu).$$

Отметим, что согласно 3.I, 3.2 при доказательстве существования однократных (экспоненциально) диофантовых представлений наравне с операциями сложения, умножения (и возведения в степень) и предикатом равенства можно использовать другие операции и предикаты, однократная представимость которых уже была установлена.

3.3. Если формулы $(\exists z_1 \dots z_\varkappa)[S = 0]$ и $(\exists y_1 \dots y_\nu)[T = 0]$ однократно представляют предикаты $\mathcal{P}(a_1, \dots, a_\iota, b_1, \dots, b_\lambda)$ и $Q(a_1, \dots, a_\iota, c_1, \dots, c_\mu)$ соответственно, и

$$\forall a_1 \dots a_\iota\ b_1 \dots b_\lambda\ c_1 \dots c_\mu \big[\neg(\mathcal{P}(a_1, \dots, a_\iota, b_1, \dots, b_\lambda) \& \& Q(a_1, \dots, a_\iota, c_1, \dots, c_\mu))\big], \tag{4}$$

то формула

$$(\exists z_1 \dots z_\varkappa\ y_1 \dots y_\nu)[(S^2 + y_1^2 + \dots + y_\nu^2)(T^2 + z_1^2 + \dots + z_\varkappa^2) = 0]$$

однократно представляет предикат

$$\mathcal{P}(a_1, \dots, a_\iota, b_1, \dots, b_\lambda) \vee Q(a_1, \dots, a_\iota, c_1, \dots, c_\mu). \tag{5}$$

Отметим, что из основной теоремы следует, что если предикаты $\mathcal{P}$ и Q имеют однократные экспоненциально диофантовы представления, то предикат (5) также имеет однократное экспоненциально диофантово представление вне зависимости от того, выполнено ли условие (4); ав-

тору не известно более прямое доказательство этого факта.

3.4. Предикаты $a<b$, $a\le b$, $a\mid b$, $a=\mathrm{rem}(b,c)$, $a=\mathrm{entier}(b/c)$, $a\equiv b(\bmod c)$, $a=\binom{b}{c}$, $a=b!$, $a=\prod_{i=0}^{b-1}(c-i)$, $a=\prod_{i=0}^{b-1}(1+ci)$ имеют однократные экспоненциально диофантовы представления.

Действительно, для первых шести предикатов можно легко указать даже однократные диофантовы представления. Остальные четыре предиката однократно представимы следующими четырьмя формулами соответственно:

$$(\exists g h w)[(w+1)^b=gw^{c+1}+aw^c+h\,\&\,w=2^b+1\,\&\,a<w\,\&\,h<w^c]$$

(это представление наиболее близко к представлению того же предиката из [3], стр.201; основная идея восходит к работе [15], различные другие варианты см. в [4], [5], [6], [12], [13], [16]);

$$(\exists k\ell n)[a=\mathrm{entier}(k/\ell)\,\&\,k=n^b\,\&\,\ell=\binom{n}{b}\,\&\,n=(2b+1)^{b+1}]$$

(это представление основано на формуле (5.3) из [15], различные модификации см. в [4], [5], [6], [13], [16]);

$$(\exists pq)[a=pq\,\&\,p=b!\,\&\,q=\binom{c}{b}];$$

$$(\exists\, de p)[[c=0\,\&\,a=1\,\&\,d=e=p=1]\vee[c>0\,\&\,a\equiv c^b\prod_{i=0}^{b-1}(e-i)(\bmod p)\,\&$$

$$\&\,e=d+b-1\,\&\,cd\equiv 1(\bmod p)\,\&$$

$$\&\,p=(1+c(b+1)^{b+1}]]$$

(это представление основано на идее, изложенной в [17]; первоначальное экспоненциально диофантово представление этого предиката, данное в [12], являлось более сложным; различные модификации см. в [4], [5], [13], [16]).

3.5. Определим полиномы $I_1, I_2, \ldots$ с рациональными коэффициентами следующим образом:

$$I_1(x_1)=x_1,$$

$$I_2(x_1, x_2) = \frac{1}{2}((x_1 + x_2)^2 + 3x_1 + x_2),$$

$$I_{n+1}(x_1, \ldots, x_n) = I_2(I_n(x_1, \ldots, x_n), x_{n+1}), \quad n = 2, 3, \ldots .$$

Хорошо известно (см., например, [I6] , § 3), что полином I_n взаимно однозначно отображает множество всех упорядоченных наборов из n натуральных чисел на множество всех натуральных чисел. Это определяет некоторое полное упорядочение таких наборов, а именно, будем говорить, что набор $\langle a_1, \ldots, a_n \rangle$ предшествует набору $\langle b_1, \ldots, b_n \rangle$, если номер первого, то есть число $I_n(a_1, \ldots, a_n)$, меньше номера второго. Отметим также, что полиномы $I_1, I_2, \ldots$ строго монотонны по каждому из своих аргументов.

3.6. Усиленная теорема Дейвиса.

Для любого перечислимого предиката $P(a_1, \ldots, a_\lambda)$ можно построить полином D и полином E, имеющий лишь неотрицательные коэффициенты, такие, что

$$P(a_1, \ldots, a_\lambda) \Longleftrightarrow (\exists x)(\forall y_{\le x})(\exists u_0 \ldots u_n)\mathcal{R}$$

$$\Longleftrightarrow (\exists x)(\forall y_{\le x})(\exists u_{0 \le E(a_1, \ldots, a_\lambda, x)} \ldots u_{n \le E(a_1, \ldots, a_\lambda, x)})\mathcal{R}$$

$$\Longleftrightarrow (\exists! x)(\forall y_{\le x})(\exists u_0 \ldots u_n)\mathcal{R}$$

$$\Longleftrightarrow (\exists x)(\forall y_{\le x})(\exists! u_0 \ldots u_n)\mathcal{R},$$

где $\mathcal{R}$ обозначает формулу

$$D(a_1, \ldots, a_\lambda, x, y, u_0, \ldots, u_n) = 0.$$

ДОКАЗАТЕЛЬСТВО. Пусть $P(a)$ – произвольный перечислимый предикат, а

$$(\exists z_1 \ldots z_n)[M(a, z_1, \ldots, z_n) = 0]$$

– его диофантово представление.

Легко видеть, что

$$P(a) \Longleftrightarrow (\exists x)(\forall y_{\le x})(\exists u_1 \ldots u_n)[y = I_n(u_1, \ldots, u_n) \,\&$$

$$\&\,[[y < x \,\&\, M(a, u_1, \ldots, u_n) \neq 0] \vee$$

$$\vee\,[y = x \,\&\, M(a, u_1, \ldots, u_n) = 0]]].$$

Действительно, если число a удовлетворяет предикату $\mathcal{P}$, то в качестве x можно взять номер первого набора $\langle z_1, \ldots, z_n \rangle$, удовлетворяющего условию

$$M(a, z_1, \ldots, z_n) = 0,$$

и только это число; при любом y, не превосходящем x, в качестве $u_1, \ldots, u_n$ можно брать тот единственный набор, номером которого является x, и только его.

Нетрудно проверить, что в качестве $\mathcal{D}$ можно взять полином

$$2^{2^n}(y - I_n(u_1, \ldots, u_n))^2 + ((x-y)M^2(a, u_1, \ldots, u_n) - 1 - u_0)^2((x-y)^2 + M^2(a, u_1, \ldots, u_n) + u_0^2),$$

а в качестве E - полином $x(1 + \tilde{M}(a, x))$, где $\tilde{M}(a, x)$ - полином, который получается из полинома $M^2(a, z_1, \ldots, z_n)$ заменой всех знаков $-$ на $+$ и подстановкой вместо $z_1, \ldots, z_n$ переменной x.

Теорема доказана.

3.7. Усиленная форма китайской теоремы об остатках.

Каковы бы ни были попарно взаимно простые положительные числа $d_1, \ldots, d_\tau$ и целые числа $\alpha_1, \ldots, \alpha_\tau$ существует ровно одно целое число a такое, что $0 \le a < d_1 \ldots d_\tau$ и $a \equiv \alpha_\iota \pmod{d_\iota}$ при $\iota = 1, \ldots, \tau$.

Легко видеть, что в качестве a можно взять остаток от деления числа a' на $d_1 \ldots d_\tau$, где a' - произвольное число, удовлетворяющее условию $a' \equiv \alpha_\iota \pmod{d_\iota}$ (существование такого a' утверждает обычная форма китайской теоремы об остатках). Можно также дать сразу доказательство теоремы в усиленной форме, следуя некоторым традиционным доказательствам (например, варианту из [6]).

Завершим доказательство основной теоремы (сформулированной в п.2). Пусть $\mathcal{P}(a)$ - произвольный перечислимый предикат, $\mathcal{D}$ и E - полиномы, существование которых утверждается в теореме п.3.6. Положим

$$\mathcal{R}(a, x, \tau, u_0, \ldots, u_n) = \sum_{\iota=0}^{\sigma} \mathcal{D}_\iota(a, x, u_0, \ldots, u_n)(-\tau)^{\sigma-\iota},$$

где $\mathcal{D}_\iota$ - такие полиномы, что

$$\mathcal{D}(a, x, y, u_0, \ldots, u_n) = \sum_{\iota=0}^{\sigma} \mathcal{D}_\iota(a, x, u_0, \ldots, u_n)(y+1)^\iota.$$

Обозначим через $F(a, x)$ полином, который получается из полинома

$D(a, x, y, u_0, \ldots, u_n)$ заменой всех знаков $-$ на знак $+$ и подстановкой вместо $y, u_0, \ldots, u_n$ полинома $x + E(a, x)$. Покажем, что предикат (a) однократно представим формулой

$$(\exists x\, r\, q\, s_0 \ldots s_n)[\mathfrak{A}_1 \,\&\, \mathfrak{A}_2 \,\&\, \mathfrak{A}_3 \,\&\, \mathfrak{A}_4], \tag{6}$$

где

$$\mathfrak{A}_1 \rightleftharpoons r = (E(a, x) + F(a, x) + x + 1)!,$$

$$\mathfrak{A}_2 \rightleftharpoons q = \prod_{i=0}^{x} (1 + r(i+1));$$

$$\mathfrak{A}_3 \rightleftharpoons \&_{\tau=0}^{n} \Big[q \Big| \prod_{i=0}^{E(a,x)} (s_\tau - i) \,\&\, s_\tau < q\Big],$$

$$\mathfrak{A}_4 \rightleftharpoons \mathcal{R}(a, x, r, s_0, \ldots, s_n) \equiv 0 \pmod{q}.$$

Доказательство будет состоять из трех частей – в п.3.8. будет показано, что (6) влечет $\mathcal{P}(a)$, в п.3.9 будет установлена справедливость обратной импликации, в п.3.10 будет доказана однократность представления (6).

3.8. Пусть $r, q, s_0, \ldots, s_n$ – числа, существование которых утверждается в формуле (6), y – произвольное число, не превосходящее x. Обозначим через p произвольный простой делитель числа $1 + r(y+1)$. Из $\mathfrak{A}_2$ и $\mathfrak{A}_3$ следует, что при $\tau = 0, \ldots, n$

$$p \Big| \prod_{i=0}^{E(a,x)} (s_\tau - i),$$

следовательно, существуют числа $u_0, \ldots, u_n$ такие, что

$$p | s_\tau - u_\tau, \quad u_\tau \le E(a, x) \quad (\tau = 0, \ldots, n). \tag{7}$$

Из $\mathfrak{A}_2$, $\mathfrak{A}_4$ и (7) следует, что

$$\mathcal{R}(a, x, r, u_0, \ldots, u_n) \equiv 0 \pmod{p}.$$

Отсюда получаем, что

$$0 \equiv \mathcal{R}(a, x, r, u_0, \ldots, u_n)$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, u_0, \ldots, u_n)(-r)^{\sigma - i}$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, u_0, \ldots, u_n)(-r)^{\sigma - i}(y+1)^{\sigma}$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, u_0, \ldots, u_n)(y+1)^{i}$$

$$\equiv D(a, x, y, u_0, \ldots, u_n) \pmod{p}.$$

Так как из $\mathcal{A}_1$ и (5) следует, что

$$p > F(a, x) \geq |D(a, x, y, u_0, \ldots, u_x),$$

то

$$D(a, x, y, u_0, \ldots, u_{\varkappa}) = 0.$$

Отсюда согласно первой эквивалентности теоремы п.3.6 следует, что имеет место (a).

3.9. Пусть a – число, удовлетворяющее предикату $\mathcal{P}$. Найдем согласно второй эквивалентности теоремы п.3.6 числа x, $u_{0,y}, \ldots, u_{\varkappa,y}$ такие, что при $y = 0, \ldots, x$

$$u_{\tau,y} \leq E(a, x) \quad (\tau = 0, \ldots, \varkappa),$$

$$D(a, x, y, u_{0,y}, \ldots, u_{\varkappa,y}) = 0. \tag{8}$$

Выберем числа r и q удовлетворяющими условиям $\mathcal{A}_1$ и $\mathcal{A}_2$. Легко проверить, что если $0 \leq y' < y'' \leq x$, то числа

$$1 + r(y' + 1), \quad 1 + r(y'' + 1) \tag{9}$$

взаимно просты. Найдем согласно п.3.7 числа $s_0, \ldots, s_{\varkappa}$ такие, что при $\tau = 0, \ldots, \varkappa$

$$s_\tau \leq q,$$

$$s_\tau \equiv u_{\tau,y} \pmod{1 + r(y+1)} \quad (y = 0, \ldots, x). \tag{10}$$

Ясно, что условие $\mathcal{A}_3$ выполнено.

Согласно (8) и (10)

$$0 \equiv D(a, x, y, s_0, \ldots, s_{\varkappa})$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, s_0, \ldots, s_{\varkappa})(y+1)^i$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, s_0, \ldots, s_{\varkappa})(y+1)^i (-r)^{\sigma}$$

$$\equiv \sum_{i=0}^{\sigma} D_i(a, x, s_0, \ldots, s_{\varkappa})(-r)^{\sigma - i}$$

$$\equiv R(a, x, r, s_0, \ldots, s_{\varkappa}) \pmod{1 + r(y+1)}.$$

Чтобы завершить обоснование свойства $\mathcal{A}_4$ достаточно вновь воспользоваться взаимной простотой чисел (9).

3.10. Пусть a – число, удовлетворяющее предикату $\mathcal{P}$. Обозначим через $\mathcal{A}'_1, \ldots, \mathcal{A}'_4$, $\mathcal{A}''_1, \ldots, \mathcal{A}''_4$ формулы, получающиеся из формул $\mathcal{A}_1, \ldots, \mathcal{A}_4$ заменой $x, r, q, s_0, \ldots, s_{\varkappa}$ на $x', r', q', s'_0, \ldots, s'_{\varkappa}$ и $x'', r'', q'', s''_0, \ldots, s''_{\varkappa}$ соответственно. По-

кажем, что из $\mathcal{U}_1' \& \ldots \& \mathcal{U}_4'$ и $\mathcal{U}_1'' \& \ldots \& \mathcal{U}_4''$ следует, что $x' = x''$, $r' = r''$, $q' = q''$, $s_0' = s_0'', \ldots, s_x' = s_x''$.

Как доказано в п.3.8, должны быть справедливы формулы

$$(\forall y_{\leq x'})(\exists u_0 \ldots u_x)[D(a, x', y, u_0, \ldots, u_x) = 0],$$

$$(\forall y_{\leq x''})(\exists u_0 \ldots u_x)[D(a, x'', y, u_0, \ldots, u_x) = 0].$$

Найдем согласно четвертой эквивалентности теоремы п.3.6 число x такое, что

$$(\forall y_{\leq x})(\exists u_0 \ldots u_x)[D(a, x, y, u_0, \ldots, u_x)]. \qquad (11)$$

Согласно третьей эквивалентности теоремы п.3.6 $x' = x'' = x$. Отсюда и из условий $\mathcal{U}_1'$, $\mathcal{U}_1''$ и $\mathcal{U}_2'$, $\mathcal{U}_2''$ получаем, что $r' = r''$, $q' = q''$; положим $r = r' = r''$, $q = q' = q''$. Не ограничивая общности будем считать, что $s_0' \neq s_0''$. Так как по условию $s_0' < q$, $s_0'' < q$, то существует простое число p и число d такие, что

$$p^d \mid q, \quad s_0' \not\equiv s_0'' \pmod{p^d}, \qquad (12)$$

и, следовательно,

$$p^d \Big| \prod_{i=0}^{E(a,x)} (s_0' - i), \qquad p^d \Big| \prod_{i=0}^{E(a,x)} (s_0'' - i).$$

Из $\mathcal{U}_1'$ и $\mathcal{U}_2'$ следует, что $p > E(a, x)$, следовательно, для некоторых чисел u_0', u_0''

$$p^d \mid s' - u_0', \qquad p^d \mid s_0'' - u_0'', \qquad (13)$$

$$u_0' \leq E(a, x), \qquad u_0'' \leq E(a, x).$$

Согласно (12) и (13) $u_0' \neq u_0''$. Найдем число y такое, что $p \mid 1 + r(y+1)$. Аналогично п.3.8, можно найти числа $u_1', \ldots, u_x'$, $u_1'', \ldots, u_x''$ такие, что

$$D(a, x, y, u_0', u_1', \ldots, u_x') = 0,$$

$$D(a, x, y, u_0'', u_1'', \ldots, u_x'') = 0.$$

Но это противоречит (11).

Основная теорема доказана.

4. Специальные формы однократных экспоненциально диофантовых представлений. Чтобы получить сформулированные во введении следствия 1 и 2, покажем, что любой перечислимый предикат $\mathcal{P}(a_1, \ldots, a_\lambda)$ однократно представим некоторой формулой вида

$$(\exists x_1 \ldots x_x y z)[z = 2^y \& D(a_1, \ldots, a_\lambda, x_1, \ldots, x_x, y, z) = 0], \qquad (14)$$

где D – полином. Этот результат близок к теореме из 3-го раздела работы М.Дейвиса [I8] – там вместо $z = 2^y$ стоит произвольный предикат экспоненциального роста, но полученное представление не является однократным. Наше доказательство будет проводиться по аналогичной схеме, основанной на свойствах последовательности решений уравнения Пелля

$$s^2 - (a^2-1)t^2 = 1 \quad (a>1); \tag{I5}$$

начало применения этих свойств для получения экзистенциальных представлений было положено Дж.Робинсон в [I5] .

Обозначим через $\langle \chi_a(n),\ \psi_a(n)\rangle$ n-ое (в порядке возрастания) решение уравнения (I5), считая $\langle 1,0\rangle$ нулевым решением. Известно (см., например, [5] , [I3] , [I5]), что последовательность $\psi_a(0),\ \psi_a(1),\ldots$ обладает следующими свойствами:

$$\psi_a(0)=0,\ \ \psi_a(1)=1,\ \ \psi_a(n+1)=2a\,\psi_a(n)-\psi_a(n-1)\ \ (n=1,2,\ldots), \tag{I6}$$

$$\psi_a(n)\equiv n \pmod{a-1} \qquad (n=0,1,\ldots). \tag{I7}$$

Из (I6) легко получить, что

$$(2a-1)^{n-1} \le \psi_a(n) \qquad (n=1,2,\ldots), \tag{I8}$$

$$\psi_a(n) \le (2a)^{n-1} \qquad (n=0,1,\ldots). \tag{I9}$$

4.I. Если $b>0$ и

$$y \ge 3(a+1)(c+1), \tag{20}$$

то

$$a = b^c \tag{2I}$$

тогда и только тогда, когда

$$a = \operatorname{entier}\left(\frac{\psi_{by+1}(c+1)}{\psi_y(c+1)}\right). \tag{22}$$

ДОКАЗАТЕЛЬСТВО. Согласно (I8) и (I9)

$$\frac{\psi_{by+1}(c+1)}{\psi_y(c+1)} \ge \frac{(2by+1)^c}{(2y)^c} \ge b^c,$$

поэтому, если выполнено или (2I), или (22), то, ввиду (20),

$$y \ge 3b^c(c+1). \tag{23}$$

Согласно (I8), (I9) и (23)

$$b^c \le \frac{(2by+1)^c}{(2y)^c} \le \frac{\psi_{by+1}(c+1)}{\psi_y(c+1)} \le$$

$$\le \frac{(2by+2)^c}{(2y-1)^c} \le b^c\left(1+\frac{3}{2y-1}\right)^c \le b^c\left(1+\frac{6c}{2y-1}\right) \le$$

$$\le b^c + \frac{6b^c c}{2y-1} < b^c + 1,$$

следовательно,

$$\operatorname{entier}\left(\frac{\psi_{by+1}(c+1)}{\psi_y(c+1)}\right) = b^c.$$

4.2. Предикат

$$\&_{i=1}^{\sigma}[a_i = b_i^{c_i}] \tag{24}$$

однократно представим формулой

$$(\exists e_1 f_1 g_1 h_1 \dots e_\sigma f_\sigma g_\sigma h_\sigma y z)[\mathcal{L}_1 \,\&\, \mathcal{L}_2 \,\&\, \&_{i=1}^{\sigma}[[b_i = 0 \,\&\, \mathcal{L}_{3,i}] \vee [b_i > 0 \,\&\, \mathcal{L}_{4,i} \,\&\, \dots \,\&\, \mathcal{L}_{7,i}]]], \tag{25}$$

где

$$\mathcal{L}_1 \rightleftharpoons y = 20 \sum_{i=1}^{\sigma} (a_i+1)(2b_i+1)(c_i^2+1),$$

$$\mathcal{L}_2 \rightleftharpoons z = 2^y,$$

$$\mathcal{L}_{3,i} \rightleftharpoons [[c_i = 0 \,\&\, a_i = 1] \vee [c_i > 0 \,\&\, a_i = 0]] \,\&\, e_i = f_i = g_i = h_i = 0,$$

$$\mathcal{L}_{4,i} \rightleftharpoons a_i = \operatorname{entier}(f_i/h_i),$$

$$\mathcal{L}_{5,i} \rightleftharpoons e_i^2 - ((b_i y+1)^2 - 1) f_i^2 = 1 \,\&\, g_i^2 - (y^2-1) h_i^2 = 1,$$

$$\mathcal{L}_{6,i} \rightleftharpoons f_i \equiv c_i + 1 (\operatorname{mod} b_i y) \,\&\, h_i \equiv c_i + 1 (\operatorname{mod} y-1),$$

$$\mathcal{L}_{7,i} \rightleftharpoons f_i < z \,\&\, h_i < z.$$

ДОКАЗАТЕЛЬСТВО. Пусть $a_1, b_1, c_1, \ldots, a_\sigma, b_\sigma, c_\sigma$ – числа, удовлетворяющие (24). Выберем числа y и z согласно $\mathcal{L}_1$ и $\mathcal{L}_2$. Если $b_\iota = 0$, то положим $e_\iota = f_\iota = g_\iota = h_\iota = 0$, тогда условие $\mathcal{L}_{3,\iota}$ будет выполнено. Если же $b_\iota > 0$, то положим

$$e_\iota = \chi_{b_\iota y+1}(c_\iota+1), \qquad f_\iota = \psi_{b_\iota y+1}(c_\iota+1),$$

$$g_\iota = \chi_y(c_\iota+1), \qquad h_\iota = \psi_y(c_\iota+1).$$

Согласно п.4.I, условие $\mathcal{L}_{4,\iota}$ выполнено. Условие $\mathcal{L}_{5,\iota}$ выполнено по определению чисел $\chi_a(n)$, $\psi_a(n)$, условие $\mathcal{L}_{6,\iota}$ – согласно (I7). Осталось проверить условие $\mathcal{L}_{7,\iota}$. Согласно (I9)

$$f_\iota \le (2b_\iota y+2)^{c_\iota} \le (y^2)^{c_\iota},$$

$$h_\iota \le (2y)^{c_\iota} \le (y^2)^{c_\iota},$$

$$y^{2c_\iota} = (\sqrt{y})^{4c_\iota} \le (2^{\sqrt{y}})^{4c_\iota} < 2^y = z.$$

Покажем теперь, что из (25) следует (24). Если $b_\iota = 0$, то должно быть выполнено $\mathcal{L}_{3,\iota}$, следовательно, $a_\iota = b_\iota^{c_\iota}$ и $e_\iota = f_\iota = g_\iota = h_\iota = 0$. Если же $b_\iota > 0$, то выполнены $\mathcal{L}_{4,\iota}, \ldots, \mathcal{L}_{7,\iota}$. По определению чисел $\chi_a(n)$, $\psi_a(n)$ из $\mathcal{L}_{5,\iota}$ следует, что для некоторых чисел n_1, n_2

$$e_\iota = \chi_{b_\iota y+1}(n_1), \qquad f_\iota = \psi_{b_\iota y+1}(n_1),$$

$$g_\iota = \chi_y(n_2), \qquad h_\iota = \psi_y(n_2).$$

Согласно (I7) из $\mathcal{L}_{6,\iota}$ следует, что

$$n_1 \equiv f_\iota \equiv c_\iota+1 \pmod{b_\iota y}, \qquad n_2 \equiv h_\iota \equiv c_\iota+1 \pmod{y-1}. \tag{26}$$

С другой стороны, согласно (I8) из $\mathcal{L}_{7,\iota}$ следует, что если $n_2 > 0$, то

$$2^y = z > h_\iota \ge (2y)^{n_2-1} > 8^{n_2-1} \ge 2^{n_2+1}.$$

Таким образом, $y > n_2+1$. Аналогично получается, что $y > n_1+1$. Это неравенство вместе с очевидным неравенством $y > c_\iota+2$ и сравнениями (26) дает равенства $n_1 = n_2 = c_\iota+1$. Отсюда и из $\mathcal{L}_{4,\iota}$ согласно п.4.I получаем, что $a_\iota = b_\iota^{c_\iota}$.

Из доказательства видно, что числа $e_\iota, f_\iota, g_\iota, h_\iota, \ldots, e_\sigma, f_\sigma, g_\sigma, h_\sigma, y, z$ однозначно определяются числами $a_1, b_1, c_1, \ldots, a_\sigma, b_\sigma, c_\sigma$, таким образом, представление (25) является однократным.

4.3. Каков бы ни был перечислимый предикат, любое его однократное экспоненциально диофантово представление за счет введения новых переменных легко может быть преобразовано в однократное представле-

ние, имеющее вид

$$(\exists z_1 \ldots z_{\varkappa})[\mathcal{P} \,\&\, \mathcal{D}],$$

где $\mathcal{P}$ – предикат вида (24), а $\mathcal{D}$ – диофантов предикат. Искомое представление вида (I4) получается отсюда на основе п.п.4.2, 3.I – 3.4.

4.4. Покажем теперь, как найти полиномы A и B, существование которых утверждается в следствиях I и 2 (см. Введение). При этом мы будем использовать одну идею Х.Патнама из [I9] . Найдем для какого-либо одноместного перечислимого, но не разрешимого предиката (a) однократное представление вида (I4) и обозначим через $A(a, x_1, \ldots, x_\nu)$, где $\nu = \varkappa + 2$ полином

$$(x_{\varkappa+1} + (x_{\varkappa+1} + x_{\varkappa+2})^2)(1 - D^2(a, x_1, \ldots, x_{\varkappa+1}, x_{\varkappa+1} + x_{\varkappa+2})). \qquad (27)$$

Покажем, что формула

$$(\exists x_1 \ldots x_\nu)[A(a, x_1, \ldots, x_\nu) = y + 4^y]$$

однократно представляет предикат (a). Действительно, если a удовлетворяет $\mathcal{P}$, то существуют числа $x_1, \ldots, x_{\varkappa}, y$ такие, что

$$D(a, x_1, \ldots, x_{\varkappa}, y, 2^y) = 0.$$

Положим $x_{\varkappa+1} = y$, $x_{\varkappa+2} = 2^y - y$, тогда равенство (I) будет выполнено. С другой стороны, если числа $a, x_1, \ldots, x_\nu, y$ удовлетворяют (I), то ввиду положительности правой части и неотрицательности первого сомножителя в (27) второй сомножитель должен быть положительным. Это возможно только тогда, когда

$$D(a, x_1, \ldots, x_{\varkappa}, x_{\varkappa+1} + x_{\varkappa+2}) = 0,$$

при этом

$$x_{\varkappa+1} + (x_{\varkappa+1} + x_{\varkappa+2})^2 = y + (2^y)^2,$$

откуда $x_{\varkappa+1} = y$, $x_{\varkappa+1} + x_{\varkappa+2} = 2^y$. Положив $z = 2^y$ получим, что

$$z = 2^y \,\&\, D(a, x_1, \ldots, x_{\varkappa}, y, z) = 0.$$

Таким образом, a удовлетворяет $\mathcal{P}$ и для данного a существует не более одного набора $x_1, \ldots, x_\nu, y$, удовлетворяющего (I). С другой стороны, неразрешимость предиката (a) исключает возможность общерекурсивной оценки величины решений уравнения (I).

Чтобы построить полином B , выберем какую-либо гёделевскую нумерацию одноместных частично рекурсивных функций и обозначим через $\mathcal{P}(a_1, a_2)$ предикат "функция с номером a_1 определена в точке a_1 и ее значение равно a_2 ". Найдем для предиката $\mathcal{P}(a_1, a_2)$ представление вида (I4) и обозначим через $B(a, x_0, \ldots, x_{\varkappa}, y, z)$ полином

$$(x_0 + 1)(1 - D^2(a, x_0, \ldots, x_{\varkappa}, y, z)).$$

Легко видеть, что из неравенства (2) следует, что

$$D(a, x_0, \ldots, x_{\varkappa}, y, 2^y) = 0$$

и, значит, имеет место $P(a, x_0)$. Таким образом, при любом a существует согласно определению предиката P не более одного значения x_0, при котором возможно неравенство (2), и, ввиду однократности представления (I4), не более одного набора значений $x_0, \ldots, x_{\varkappa}, y$, удовлетворяющего (2). С другой стороны, для любой одноместной общерекурсивной функции C имеет место неравенство (3) при a, равном номеру функции C, $x_0 = C(a)$ и значениях остальных переменных, выбранных согласно (I4) при $a_1 = a$, $a_2 = x_0$.

Литература

1. Thue A. Über Annäherungswerte algebraischer Zahlen."J.reine und angew. Math.", 1909, 135, 284-305.
2. Backer A. Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms. "Philos.Trans.Roy.Soc.London (A)", 1968, 263, № 1139, 173-191.
3. Матиясевич Ю.В. Диофантовы множества. "Успехи мат.наук", 1972, 27, № 5 (I67), I85-222.
4. Davis M. Hilbert's tenth problem is unsolvable. "Amer.Math. Mon.", 1973, 80, № 3, 233-269.
5. Манин Ю.И. Десятая проблема Гильберта. "Современные проблемы математики", 1973, I, 5-37.
6. Матиясевич Ю.В. Диофантово представление множества простых чисел. "Докл. АН СССР", I97I, I96, № 4, 770-773.
7. Чудновский Г.В. Некоторые арифметические проблемы. Препринт ИМ-7I-3 Ин-та матем. АН Укр.ССР, I97I.
8. Косовский Н.К. О диофантовых представлениях последовательности решений уравнения Пелля. "Зап.научн.семинаров Ленингр.отд.Матем.ин-та АН СССР", I97I, 20, 49-59.
9. Davis M. An explicit Diophantine definition of the exponential function. "Communs Pure and Appl.Math.", 1971, 24, № 2, 137-145.
10. Davis M. One equation to rule them all. "Trans. New York Acad. Sci.", Ser.II, 1968, 30, 766-773.
11. Herrmann O. On the non-trivial solution of the Diophantine equation $9(u^2+7v^2)-7(r^2+7s^2)^2=2$. Computers in number theory, "Proc.Atlas Symp.", № 2, Oxford, 1969, 207-217.
12. Davis M., Putman H., Robinson J. The decision problem for exponential Diophantine equations. "Ann.Math.",

1961, 74, № 3, 425-436 (русск.перев.: "Математика", I964, 8, № 5, 69-79).
13. Robinson J. Diophantine decision problems. Studies in number theory, "MAA Studies in Math.", 1969, 6, 76-116.
14. Davis M. Arithmetical problems and recursively enumerable predicates. "J. Symbol. Log.", 1953, 18,№ 1, 33-41 (русск.перев.: "Математика", I964, 8,№ 5, I5-22).
15. Robinson J. Enistential definability in arithmetic. "Trans. Amer.Math.Soc.", 1952, 72, № 3, 437-449 (русск.перев.: "Математика", I964, 8, № 5,3-I4)
16. Мальцев А.И. Алгоритмы и рекурсивные функции. М., I965.
17. Robinson J. Hilbert's tenth problem. "Proc.Symp.Pure Math.", 1971, 20, 191-194.
18. Davis M. Extentions and corollaries of recent work on Hilbert's tenth problem. "Ill.J.Math.", 1963, 7, № 2, 246-250 (русск.перев.: "Математика", I964, 8, 5, 80-84).
19. Putnam H. An unsolvable problem in number theory. "J.Symbol. Log.", 1960, 25, № 3, 220-232 (русск.перев.: "Математика", I964, 8, № 5, 55-67).