TUCS Seminar on Discrete Mathematics 1997.

Yuri V. Matiyasevich: Hilbert's Tenth Problem,
The MIT Press, Cambridge, Massachusetts 1993.

Hilbert's tenth problem is reprinted in: "Mathematical developments arising form Hilbert problems" (Proceedings of Symposia in Pure Mathematics, American Mathematical Society, Providence, Rhode Island, 1976) and translated as

10. Determination of the Solvability of a Diophantine Equation.

Given a diophantine equation with any number of unknown quantities and with rational integer numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations wheter the equation is solvable in rational integers.*

Preliminaries

The set of natural numbers here is $\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z}_+ = \mathbb{N} \setminus \{0\}$, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Diophantine equation is of form

$$D(x_1, \dots, x_m) = 0, \tag{1.1.1}$$

where $D(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$. Sometimes form

$$D_L(x_1, \dots, x_m) = D_R(x_1, \dots, x_m), \tag{1.1.2}$$

Where $D_L(x_1, \dots, x_m), D_R(x_1, \dots, x_m) \in \mathbb{Z}_+[x_1, \dots, x_m]$ is preferrable.

System

$$\begin{cases} D_1(x_1, \dots, x_m) & = 0 \\ \dots & \\ D_k(x_1, \dots, x_m) & = 0 \end{cases} \tag{1.2.1}$$

has an integer solution if and only if the Diophantine equation

$$D_1^2(a_1, \dots, x_m) + \dots + D_k^2(x_1, \dots, x_m) = 0 \tag{1.2.2}$$

has one.

We will call two systems of Diophantine equations (solvability) equivalent, if they have the same solvability status.

Introducing new variables any Diophantine equation can be tranformed into an equivalent system consisting of equations of forms

$$\alpha = \beta + \gamma$$

and

$$\alpha = \beta\gamma,$$

where α, β and γ are either natural numbers or variables. Take, for instance

$$4x^2y - 5x^3 + 2y = 0.$$

Transposing the negative terms we get

$$4x^2y + 2y = 5z^3.$$

Substituting $r_1 = 4x$, $s_1 = 2y$, $t_1 = 5z$ we get

$$r_1xy + s_1 = t_1z^2.$$

Continuing this way, $r_2 = r_1x$, $t_2 = t_1z$, we have

$$r_2y + s_1 = t_2z.$$

Furthermore, letting $r_3 = r_2y$ and $t_3 = t_2z$ the equation becomes

$$r_3 + s_1 = t_3.$$

Finally substituting $q_1 = r_3 + s_1$ we see that the original equation is equivalent to system

$$\begin{cases} r_1 = 4x & r_2 = r_1x & r_3 = r_2y \\ t_1 = 5z & t_2 = t_1z & t_3 = t_2z \\ s_1 = 2y & q_1 = r_3 + s_1 & q_1 = t_2 \end{cases}$$

We conclude that each Diophantine equation is (solvability) equivalent to a Diophantine equation of degree four.

Open problem: Is the restriction of Hilbert's Tenth problem to equations of degree 3 undecidable?

Solutions in natural numbers

Let p be an odd prime number. Then the Diophantine equation

$$(x+1)^p + (y+1)^p = (z+1)^p$$

has infinitely many solutions of form $x = z$, $y = -1$, but it has no natural number solutions (Wiles 1995).

Let

$$D(x_1, \ldots, x_m) = 0 \tag{1.3.2}$$

be an arbitrary Diophantine equation. Any solution of system

$$\begin{cases} & D(x_1, \ldots, x_m) = 0 \\ x_1 & = y_{11}^2 + y_{12}^2 + y_{13}^2 + y_{14}^2 \\ & \ldots \\ x_m & = y_{m1}^2 + y_{m2}^2 + y_{m3}^2 + y_{m4}^2 \end{cases} \tag{1.3.3}$$

is clearly an integer solution of (1.3.2), but since any natural number can be expressed as a sum of four squares, also any solution of (1.3.2) yields a solution of (1.3.3). System (1.3.3) can be compressed into a single equation

$$E(x_1, \ldots, x_m, y_{11}, \ldots, y_{m4}) = 0 \tag{1.3.4}$$

that is solvable in integers if and only if (1.3.2) is solvable in natural numbers.

We have seen that it suffices to establish the unsolvability of Hilbert's Tenth Problem for solutions in natural numbers.

For this on, latin letters a, b, c, ... will stand for natural numbers, unless explicitely otherwise stated.

Families of Diophantine equations

Let D be a polynomial with integer coefficients with variables a_1, ..., a_n, x_1, ..., x_n. Fixing parameters a_1, ..., a_n in equation

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{1.4.1}$$

yields a particular equation in a family of Diophantine equations. The parametric equation (1.4.1) defines a set $\mathfrak{M}$ that consists of those n-tuples $(a_1, \ldots, a_n)$ for which (1.4.1) has a solution in natural numbers:

$$(a_1, \ldots, a_n) \in \mathfrak{M} \iff \exists x_1, \ldots, x_m \, [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]. \tag{1.4.2}$$

Eqivalence (1.4.2) is a *Diophantine representation* of $\mathfrak{M}$. Any subset of $\mathbb{N}^n$ that has a Diophantine representation, is called a *Diophantine set of dimension* n. Clearly there are infinitely many Diophantine representations for a Diophantine set.

If $A \subseteq \mathbb{N}^a$ and $f : A \to \mathbb{N}$ is a function and set

$$\{(f(x_1, \ldots, x_n), x_1, \ldots, x_n) \mid (x_1, \ldots, x_n) \in A\}$$

is a Diophantine set, we say that f is a *Diophantine function*. In the same manner, we define a *Diophantine relation*.

No restrictions were imposed on the equation (1.4.1), but as we have seen, we could require that (1.4.1) should be an equation of degree four.

EXAMPLES. Set E of even numbers is Diophantine:

$$a \in E \iff \exists x\,[2x = a].$$

We will also say that property "is an even number" is Diophantine and denote

$$\text{Even}(a) \iff \exists x\,[2x = a]$$

Relation $\{(a, b) \in \mathbb{N}^2 \mid a \neq b\}$ is Diophantine:

$$a \neq b \iff \exists x[(a - b)^2 = x + 1].$$

Union and intersection of Diophantine sets of the same dimension is also Diophantine: If

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) = 0$$

and

$$D_2(a_1, \ldots, a_n, x_1, \ldots, x_{m_2}) = 0$$

define Diophantine representations for two sets, then the equation

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) \cdot D_2(a_1, \ldots, a_n, x_1, \ldots, x_{m_2}) = 0$$

yields a Diophantine representation for their union and

$$D_1^2(a_1, \ldots, a_n, x_1, \ldots, x_{m_1}) + D_2^2(a_1, \ldots, a_n, y_1, \ldots, y_{m_2}) = 0$$

gives the required representation for the intersection.

Equation

$$D(a, x_1, \ldots, x_m) = 0$$

has a solution x_1, ..., x_m if and only if the equation

$$(x_0 + 1)(1 - D^2(x_0, \ldots, x_m)) - 1 = a$$

has a solution in unknowns x_0, ..., x_m. Therefore, a set of natural numbers is Diophantine if and only if it is the set of all natural number values assumed by some polynomial with integer coefficients for natural number values of its variables.

Generalized Diophantine representations

Let P be a polynomial with integer coefficients. We handle also equations of form

$$P(\mathfrak{t}_1, \ldots, \mathfrak{t}_k) = 0, \tag{1.5.7}$$

where $\mathfrak{t}_1$, ..., $\mathfrak{t}_k$ are Diophantine terms, that is, expressions constructed in the natural manner from variables, natural numbers, symbols "+", "-", "·"and symbols for Diophantine functions. To be precise, we define the Diophantine terms to be the smallest set that satisfies the following:

1) Natural numbers and variable symbols are Diophantine terms.

2) If $\mathfrak{t}_1$ and $\mathfrak{t}_2$ are Diophantine terms, then also $\mathfrak{t}_1 + \mathfrak{t}_2$, $\mathfrak{t}_1 - \mathfrak{t}_2$ and $\mathfrak{t}_1\mathfrak{t}_2$ are Diophantine terms.

3) If F is a Diophantine function and $\mathfrak{t}_1$, ..., $\mathfrak{t}_k$ Diophantine terms, then also $F(\mathfrak{t}_1, \dots, \mathfrak{t}_k)$ is a Diophantine term.

Inductively, introducing new variables, we can obtain a system of equations of forms (1.2.5), (1.2.6) and

$$\alpha = F(\beta_1, \dots, \beta_n), \tag{1.5.8}$$

where F is a Diophantine function and α, β_1, ..., β_n variables or natural numbers, that has a solution if and only if (1.5.7) has.

Moreover, we can replace each equation (1.5.8) by

$$\alpha = F(\beta_1, \dots, \beta_n) \iff \exists y_1 \dots y_m \, [D(\alpha, \beta_1, \dots, \beta_n, y_1, \dots, y_m) = 0], \tag{1.5.6}$$

where D gives the Diophantine representation of F and $y_1, \dots, y_m$ are new variables that has not yet beem used. The resulting system can then be compressed into a single equation equivalent to (1.5.7).

In generalized Diophantine equations we will also use symbols & and $\vee$ for the intersection and union of Diophantine relations:

$$\mathcal{R}(a_1, \dots, a_n) \iff \exists x_1, \dots, x_m \, [D(a_1, \dots, a_n, x_1, \dots, x_m) = 0]$$

is called a Diophantine representation of relation $\mathcal{R}$. If $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine relations of same dimensions, then

$$\mathcal{R}(a_1, \dots, a_n) \iff \mathcal{R}_1(a_1, \dots, a_n) \vee \mathcal{R}_2(a_1, \dots, a_n)$$

and

$$\mathcal{S}(a_1, \dots, a_n) \iff \mathcal{R}_1(a_1, \dots, a_n) \,\&\, \mathcal{R}_2(a_1, \dots, a_n)$$

are the generalized Diophantine representations for their union and intersection respectively. We have seen that both of them also have the genuine Diophantine representation.

If $\mathcal{R}$ is a Diophantine relation and $\mathfrak{t}_1$, ..., $\mathfrak{t}_n$ Diophantine terms, then generalized Diophantine assertion is equivalent to

$$\exists t_1, \dots r_n [\mathcal{R}(t_1, \dots, t_n) \,\&\, t_1 = \mathfrak{t}_1 \,\&\, \dots \,, \,\&\, t_n = \mathfrak{t}_n].$$

Examples. Property Even(a) has a genuine Diophantine representation:

$$\text{Even}(a) \iff \exists x \, [2x = a].$$

Property Odd(a) has a generalized Diophantine representation

$$\text{Odd}(a) \iff \text{Even}(a + 1),$$

but also a genuine Diophantine representation:

$$\text{Odd}(a) \iff \exists x \, [2x + 1 = a].$$

Then

$$\text{Even}(a) \iff \text{Odd}(a + 1)$$

is a generalized Diophantine representation.

Some Diophantine sets, properties, relations, and functions

We have seen that relation $\neq$ is Diophantine in $\mathbb{N}^2$. We have also

$$\begin{aligned} a \leq b &\iff \exists x\,[a + x = b], \\ a < b &\iff \exists x\,[a + x + 1 = b], \text{ and} \\ a \mid b &\iff \exists x[ax = b] \end{aligned}$$

A generalized Diophantine representation for the congruence with respect to a positive modulus is given by

$$a \equiv b \pmod{c} \iff c \mid (b - a).$$

The function "remainder on dividing b by c" has a generalized Diophantine representation:

$$a = \mathrm{rem}(b, c) \iff a < c \,\&\, b \equiv a \pmod{c}.$$

Function $\mathrm{arem}(b, c)$ is the least absolute value $|\chi|$ among all numbers χ congruent to b with respect to modulus c, that is,

$$\mathrm{arem}\,(b, c) \equiv \pm b \text{ arem } 0 \leq \mathrm{arem}(b, c) \leq \frac{c}{2}.$$

Function $\mathrm{arem}(b, c)$ is Diophantine:

$$a = \mathrm{arem}\, b, c \iff 2a \leq c \,\&\, [c \mid (b - a) \vee c \mid (b + a)].$$

Also, non-divisibility is Diophantine:

$$a \nmid b \iff \mathrm{rem}(b, a) > 0.$$

In the semiring of natural numbers we cannot speak about proper division, but the integer part of b/c, written as b div c can be well defined and is a Diophantine function:

$$a = b \text{ div } c \iff ac + \mathrm{rem}(b, c) = b.$$

Greatest common divisor:

$$a = \gcd(b, c) \iff bc > 0 \,\&\, a \mid b \,\&\, a \mid c \,\&\, [\exists xy\,[a = bx - cy] \vee \exists xy\,[a = cy - bx]]\,.$$

Least common multiple:

$$a = \mathrm{lcm}(b, c) \iff bc = a \gcd(b, c).$$

Exponentiation is Diophantine

The aim is to show that set of triples

$$\{(a, b, c) \mid a = b^c\}$$

is Diophantine. If that holds, then also the set

$$\{(a, b) \mid \exists n\, [a = b^n]\}$$

would be Diophantine. We can consider the powers of b as the set of all members of the first-order recurrent sequence

$$\beta_b(0) = 1, \quad \beta_b(n+1) = b\beta_b(n).$$

The proof here will utilize the recurrent sequence

$$\alpha_b(0) = 0, \quad \alpha_b(1) = 1, \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n). \tag{2.1.4}$$

We will try to show that the set

$$\{a, b, c) \mid b \geq 4, \,\&\, a = \alpha(b)\}$$

is Diophantine. It is immediate that $\alpha_b(n)$ is a monotonously growing and $\alpha_b(n) \geq n$. For a fixed n and large b the function $\alpha_b(n)$ behaves much like b^n, indeed by induction we get

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n.$$

The assertion is clear for $n = 0$. We have

$$\alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \leq b\alpha_b(n+1) \leq b \cdot b^n = b^{n+1}$$

and

$$\begin{aligned}
\alpha_b(n+2) &= b\alpha_b(n+1) - \alpha_b(n) \\
&\geq b\alpha_b(n+1) - \alpha_b(n+1) \\
&= (b-1)\alpha_b(n+1) \geq (b-1)(b-1)^b \\
&= (b-1)^{n+1}.
\end{aligned}$$

We shall see that

$$b^c = \lim_{x \to \infty} \frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)},$$

and the limit number for x can be expressed using function α_b. Using this knowledge we see that

$$b^c = \alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1),$$

when x is large enough.

We will begin with set

$$\{(a, b) \mid b \geq 2 \,\&\, \exists n\, [a = \alpha_b(n)]\} \tag{2.1.5}$$

and show that it is Diophantine. Now, the recurrence relation can be expressed using matrices (with $\alpha_b(-1) = -1$).

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \text{ and } \Xi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}.$$

We see that $A_b(0) = I$, $A_b(n+1) = A_b(n)\Xi_b$, which implies that

$$A_b(n) = \Xi_b^n.$$

Therefore, $\det(A_b(n)) = 1$ for each n, which means that

$$\begin{aligned} 1 &= -\alpha_b(n)\alpha_b(n-1) + \alpha_b^2(n) \\ &= \alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) \\ &= \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n) \end{aligned}$$

We will see that if

$$x^2 - bxy + y^2 = 1, \tag{2.1.12}$$

then x and y are consequtive members of the sequence (2.1.4), that is, either

$$x = \alpha_b(m+1), \quad y = \alpha_b(m) \tag{2.1.13}$$

or

$$x = \alpha_b(m), \quad y = \alpha_b(m+1). \tag{2.1.14}$$

Moreover, if we require (2.1.12) and $y < x$, it turns out that there will be m such that (2.1.13) hodls. This is proved by induction on y. If $y = 0$, then we have $x = 1$, so (2.1.13) holds with $m = 0$. Let $y > 0$. then we have

$$x = \frac{1 - y^2}{x} + by \leq by \tag{2.1.17}$$

and

$$x = \frac{1}{x} - \frac{y^2}{x} + by > by - y. \tag{2.1.18}$$

Let $x_1 = y$ and $y_1 = by - x$. Then $y_1 < x_1$ and direct calculation gives

$$x_1^2 - bx_1y_1 + y_1^2 = 1.$$

By the induction hypothesis, there exists m_1 such that

$$x_1 = \alpha_b(m_1 + 1) \text{ and } y_1 = \alpha_b m_1 \tag{2.1.20}$$

Letting $m = m_1 + 1$ we have

$$x = bx_1 - y_1 = \alpha_b(m+1) \text{ and } y = x_1 = \alpha_b(m),$$

which proves tha claim.

The special recurrent sequences are Diophantine

The next goal is to show that

$$\{(a,b,c) \mid b \geq 4 \,\&\, a = \alpha_b(c)\} \tag{2.2.1}$$

Is Diophantine. The set (2.2.1) can be considered as the union of the termis of the sequences

$$(\alpha_b(0), b, 0), \ldots, (\alpha_b(n), b, n). \tag{2.2.2}$$

for $b \geq 4$. Using induction on (2.1.4), it is easy to see that

$$\alpha_2(n) = n$$

Therefore, for $b = 2$ the sequence (2.2.2) is

$$(0,2,0), \ldots, (n,2,n).$$

By induction it is also easy to see that if $b_1 \equiv b_2 \pmod{q}$, then

$$\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \pmod{q}. \tag{2.2.5}$$

Particulary,

$$\alpha_b(n) \equiv \alpha_2(n) = n \pmod{b-2}, \tag{2.2.7}$$

So the first $b-2$ members of (2.2.2) coincide with the first $b-2$ memebers of the sequence

$$(\alpha_b(0), b, \mathrm{rem}(\alpha_b(0), b-2)), \ldots, (\alpha_b(n), b, \mathrm{rem}(\alpha_b(n), b-2)). \tag{2.2.8}$$

In this sequence, n occurs only as an argument of α. Since the set (2.1.5) is Diophantine and rem is a Diophantine function, also the set of triples (2.2.8) is Diophantine. But only the initial segments of (2.2.2) and (2.2.8) are equal. Let then

$$w \equiv b \pmod{v} \tag{2.2.9}$$

$$w \equiv 2 \pmod{u} \tag{2.2.10}$$

$$v > 2\alpha_b(k) \tag{2.2.11}$$

$$u > 2k \tag{2.2.12}$$

and $n \leq k$. Then $2\alpha_b(n) \leq 2\alpha_b(k) < v$ and $\alpha_w(n) \equiv \alpha_b(n) \pmod{v}$, so we conclude that

$$\alpha_b(n) = \mathrm{arem}(\alpha_w(n), v).$$

Moreover, $2n \leq 2k < u$ and $\alpha_w(n) \equiv \alpha_2(n) = n \pmod{u}$. Therefore also $\mathrm{arem}(\alpha_w(n), u) = n$. We have then a sequence

$$(\mathrm{arem}(\alpha_w(0), v), b, \mathrm{arem}(\alpha_w(0), u))), \ldots, \\ \ldots, (\mathrm{arem}(\alpha_w(n), v), b, \mathrm{arem}(\alpha_w(n), u))), \ldots \tag{2.2.13}$$

where k first terms equal to those one of (2.2.2). The union of sequences (2.2.13) where u, v and w satisfy (2.2.9) and (2.2.10) certainly contains all triples of (2.2.2). However, there may be some additional triples.

We will now study the recurrent relation to understand the occurrence of the extra triples. Let

$$v = \alpha_b(m+1) - \alpha_b(m-1). \tag{2.2.16}$$

Then

$$\alpha_b(m+1) \equiv \alpha_b(m-1) \pmod{v}, \tag{2.2.17}$$

and because the recurrent relation can be written as

$$\alpha_b(n-2) = b\alpha_b(n-1) - \alpha_b(n), \tag{2.2.18}$$

we have

$$\begin{aligned} \alpha_b(m+2) &= b\alpha_b(m+1) - \alpha_b(m) \\ &\equiv b\alpha_b(m-1) - \alpha_b(m) \pmod{v} \\ &= \alpha_b(m-2) \end{aligned} \tag{2.2.19}$$

By induction we get also

$$\begin{aligned} \alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v} \\ &\dots \\ \alpha_b(2m-1) &\equiv \alpha_b(1) \pmod{v} \\ \alpha_b(2m) &\equiv \alpha_b(0) \pmod{v} \end{aligned} \tag{2.2.20}$$

Moreover,

$$\alpha_b(2m) \equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \tag{2.2.21}$$

and

$$\alpha_b(2m+1 = b\alpha_b(2m) - \alpha_b(2m-1) \equiv -\alpha_b(1). \pmod{v} \tag{2.2.22}$$

By induction we get

$$\alpha_b(2m+n) \equiv -\alpha_b(n) \pmod{v} \tag{2.2.23}$$

So, for this choise of v (2.2.16), sequence $\alpha_b(0)$, ..., $\alpha_b(n)$, ... modulo v has the following period of $4m$ terms:

$$\begin{aligned} &0,\ 1,\dots,\ \alpha_b(m-1),\ \alpha_b(m),\ \alpha_b(m-1),\dots,\ 1, \\ &0,-1,\dots,-\alpha_b(m-1),-\alpha_b(m),-\alpha_b(m-1),\dots,-1. \end{aligned} \tag{2.2.24}$$

But this is also the period modulo v of the sequence

$$\alpha_w(0), \dots, \alpha_w(n), \dots \tag{2.2.25}$$

Because

$$\begin{aligned} v &= \alpha_b(m+1) - \alpha_b(m-1) \\ &= b\alpha_b(m) - 2\alpha_b(m-1) \\ &\geq 2\alpha b(m) \end{aligned}$$

for $b \geq 4$, also the sequence

$$\operatorname{arem}(\alpha_w(0), v), \ldots, \operatorname{arem}(\alpha_w(n), v) \tag{2.2.26}$$

has the period of $2m$ terms

$$0, 1 \ldots, \alpha_b(m-1), \alpha_b(m), \alpha_b(m-1), \ldots, 1. \tag{2.2.27}$$

Now (2.2.10) implies that the sequence (2.2.25) modulo u has the period of u terms

$$0, 1, \ldots, u-1. \tag{2.2.28}$$

Introducing the condition

$$u \mid m \tag{2.2.29}$$

we guarantee that the length of the period of the sequence (2.2.26) is a multiple of the length of the period of the sequence

$$\operatorname{arem}(\alpha_w(0), u), \ldots \operatorname{arem}(\alpha_w(n), u), \ldots \tag{2.2.30}$$

Therefore, the extra triples in (2.2.13) will appear among the $m+1$ members (this is an almost symmetric period) of this sequence. For these initial triples codition

$$2 \operatorname{arem}(\alpha_w(n), v) < u \tag{2.2.14}$$

which can be written as

$$2\alpha_b(n) < u \tag{2.2.31}$$

implies

$$2n < u, \tag{2.2.32}$$

because

$$n \leq \alpha_b(n). \tag{2.2.33}$$

Now

$$\operatorname{arem}(\alpha_w(n), u) = \operatorname{arem}(n, u) = n \tag{2.2.34,}$$

so condition (2.2.14) eliminates all extra triples. But still it is not known how to express conditions (2.2.16) and (2.2.29) without knowing that α is Diophantine. Because of this, we shall prove that

$$\alpha_b^2(k) \mid \alpha_b(m) \implies \alpha_b(k) \mid m \tag{2.2.35}$$

and replace (2.2.29) with

$$u^2 \mid \alpha_b(m). \tag{2.2.37,}$$

where

$$u = \alpha_b(k). \tag{2.2.36}$$

Let first b, k and m satisfy

$$\alpha_b^2(k) \mid \alpha_b(m). \tag{2.3.1}$$

Let

$$m = n + kl, \quad 0 \leq n < k. \tag{2.3.2}$$

Then

$$\begin{aligned}\begin{pmatrix}\alpha_b(m+1) & -\alpha_b(m)\\ \alpha_b(m) & -\alpha_b(m-1)\end{pmatrix} &= A_b(m)\\ &= \Xi_b^m\\ &= \Xi_b^{n+kl}\\ &= \Xi_b^n(\Xi_b^k)^l\\ &= A_b(n)A_b^l(k)\\ &= \begin{pmatrix}\alpha_b(n+1) & -\alpha_b(n)\\ \alpha_b(n) & -\alpha_b(n-1)\end{pmatrix}\\ &\cdot\begin{pmatrix}\alpha_b(k+1) & -\alpha_b(k)\\ \alpha_b(k) & -\alpha_b(k-1)\end{pmatrix}^l.\end{aligned} \tag{2.3.3}$$

Therefore

$$\begin{aligned}&\begin{pmatrix}\alpha_b(m+1) & -\alpha_b(m)\\ \alpha_b(m) & -\alpha_b(m-1)\end{pmatrix}\\ \equiv&\begin{pmatrix}\alpha_b(n+1) & -\alpha_b(n)\\ \alpha_b(n) & -\alpha_b(n-1)\end{pmatrix}\begin{pmatrix}\alpha_b(k+1) & 0\\ 0 & -\alpha_b(k-1)\end{pmatrix} \pmod{\alpha_b(k)}.\end{aligned} \tag{2.3.4}$$

We conclude that

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^l(k+1) \pmod{\alpha_b(k)}. \tag{2.3.5}$$

By (2.1.11) $\gcd(\alpha_b(k), \alpha_b(k+1)) = 1$, so from (2.3.1) and (2.3.5) we have

$$\alpha_b(k) \mid \alpha_b(n), \tag{2.3.6}$$

but also $\alpha_b(n) < \alpha_b(k)$. Therefore $n = 0$ and $m = kl$. Also

$$\begin{aligned}A_b(m) &= A_b^l(k)\\ &= (\alpha_b(k)\Xi_b - \alpha_b(k-1) - \alpha_b(k-1)I)^l\\ &= \sum_{i=0}^{l}(-1)^{l-i}\binom{l}{i}\alpha_b^i(k)\alpha_b^{l-i}(k-1)\Xi_b^i,\end{aligned} \tag{2.3.7}$$

which implies that

$$\begin{aligned}\alpha_b(m) &= \begin{pmatrix}\alpha_b(m+1) & -\alpha_b(m)\\ \alpha_b(m) & -\alpha_b(m-1)\end{pmatrix}\\ &\equiv (-1)^l\alpha_b^l(k-1)I + (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1)\Xi \pmod{\alpha_b^2(k)},\end{aligned} \tag{2.3.8}$$

so we have

$$\alpha_b(m) =\equiv (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1), \quad \pmod{2.3.9}$$

which implies that

$$\alpha_b(k) \mid l\alpha_b^{l-1}(k-1). \tag{2.3.10}$$

Since $\gcd(\alpha_b(k), \alpha_b(k-1)) = 1$, we have finally

$$\alpha_b(k) \mid l \tag{2.3.11}$$

$$b \geq 4 \tag{2.3.12}$$
$$u^2 - but + t^2 = 1 \tag{2.3.13}$$
$$s^2 - bsr + r^2 = 1 \tag{2.3.14}$$
$$r < s \tag{2.3.15}$$
$$u^2 \mid s \tag{2.3.16}$$
$$v = bs - 2r \tag{2.3.17}$$
$$v \mid (w - b) \tag{2.3.18}$$
$$u \mid w - 2 \tag{2.3.19}$$
$$w > 2 \tag{2.3.20}$$
$$x^2 - wxy + y^2 = 1 \tag{2.3.21}$$
$$2a < u \tag{2.3.22}$$
$$a = \operatorname{arem}(x, v) \tag{2.3.23}$$
$$c = \operatorname{arem}(x, u) \tag{2.3.24}$$

$$\begin{aligned}
(2.3.12), (2.3.13) &\implies \exists k\,[u = \alpha_b(k)] && (2.3.26)\\
(2.3.12), (2.3.14), (2.3.15) &\implies \exists m\,[s = \alpha_b(m), r = \alpha_b(m-1)] && (2.3.27)\\
(2.3.16), (2.3.26), (2.3.27) &\implies u \mid m && (2.3.28)\\
(2.3.17), (2.3.27) &\implies v = \alpha_b(m+1) - \alpha_b(m-1) && (2.3.29)\\
(2.3.20), (2.3.21) &\implies \exists n\,[x = \alpha_w(n)] && (2.3.30)\\
(2.3.18), (2.3.19) &\implies x \equiv \alpha_b(n) \pmod{v}, && (2.3.31)\\
& \qquad x \equiv n \pmod{u}. && (2.3.32)
\end{aligned}$$

If $n = 2lm \pm j$, where $j \leq m$, we have

$$\begin{aligned}
A_b(n) &= \Xi_b^n \\
&= \Xi_b^{2lm \pm j} \\
&= ((\Xi_b^m)^2)^l \Xi_b^{\pm j} \\
&= (A_b(m)^2)^l A_b(j)^{\pm 1},
\end{aligned} \tag{2.3.35}$$

$$\begin{aligned}
A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\
&\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v} \\
&= -A_b(m)^{-1},
\end{aligned} \tag{2.3.36}$$

$$A_b(m)^2 \equiv -I \pmod{v} \tag{2.3.37}$$

and

$$A_b(n) \equiv \pm A_b(j)^{\pm 1} \pmod{v} \tag{2.3.38}$$

Now

$$x \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v} \tag{2.3.39}$$

and

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v. \tag{2.3.40}$$

Therefore

$$a = \operatorname{arem}(x, v) = \operatorname{arem}(\alpha_b(n), v) = \alpha_b(j). \tag{2.3.41}$$

From (2.3.22) and (2.3.41) we have

$$2j \leq 2\alpha_b(j) = 2a < u, \tag{2.3.42}$$

Finally (2.3.28), (2.3.31), (2.3.33) and (2.3.42) imply

$$c = \operatorname{arem}(x, u) = \operatorname{arem}(n, u) = j \tag{2.3.43}$$

which gives us $a = \alpha_b(c)$.

To the other direction, we suppose that numbers a, b and c satisfy $b \geq 4$ and $a = \alpha_b(c)$. We should show that there are numbers r, s, t, u, v and w that satisfy (2.3.13)-(2.3.24). We will choose k and u such that (2.3.22) and (2.3.26) hold and u is odd. r and s will are chosen to satisfy (2.3.27) with $m = uk$. Now both (2.3.14) and (2.3.15) both hold. Because

$$s = \alpha_b(uk) \equiv (-1)^{u-1} u \alpha_b(k) \alpha_b^{u-1}(k-1) \pmod{u^2}, \tag{2.3.46}$$

so (2.3.16) also holds.

$$bs - 2r \geq 4\alpha_b(m) - 2\alpha_b(m-1) > 2\alpha_b(m),$$

so we can choose v such that (2.3.17) will hold. Then $\gcd(u, v) = 1$ since if $d \mid u$ and $d \mid v$, then (2.3.16) implies that $d \mid s$ and from (2.3.17) $d \mid 2r$. However, u was chosen to be odd and therefore d also is odd, so $d \mid r$ and $d \mid 1$ by (2.3.14). By the Chinese Remainder Theorem w satisfying (2.3.18), (2.3.19) and (2.3.20) can be found. Let then

$$x = \alpha_w(c) \equiv \alpha_b(c) = a \pmod{v} \tag{2.3.49}$$

Now $v > 2a$ by (2.3.17), (2.3.25) and (2.3.47), so (2.3.23) is valid. By (2.2.7) it follows that

$$x \equiv c \pmod{w-2} \tag{2.3.51}$$

and (2.3.19) guarantees that also

$$x \equiv c \pmod{u}. \tag{2.3.52}$$

Because

$$2c \leq 2\alpha_b(c) = 2a < u$$

by (2.2.33), (2.3.25) and (2.3.22), so (2.3.24) holds.

Exponentiation is Diophantine

We recall that

$$(b-1)^n \le \alpha_b(n+1) \le b^n \tag{2.4.1}$$

and will show that

$$b^c = \lim_{x\to\infty} \frac{\alpha_{bx+c}(c+1)}{\alpha_x(c+1)} \tag{2.4.2}$$

It is easily seen that

$$\frac{\alpha_{bx+c}(c+1)}{\alpha_x(c+1)} \ge \frac{(bx+3)^c}{x^c} \ge b^c, \tag{2.4.3}$$

so if (2.4.2) holds, then for large x we have

$$b^2 = \alpha_{bx+4}(c+1) \text{ div } \alpha_x(c+1). \tag{2.4.4}$$

For $b = c = 0$, $x \ge 4$ we have

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} = 1 \tag{2.4.5}$$

and for $b = 0$, $c > 0$, $x > 4$ we have

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} < \frac{4^c}{(x-1)^c} \le 1. \tag{2.4.6}$$

For $b > 0$, $x > 16c$ we have

$$\begin{aligned}
\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)} &\le \frac{(bx+4)^c}{(x-1)^c} \\
&\le \frac{(1+\frac{4}{x})^c}{(1-\frac{1}{x})^c} b^c \\
&\le \frac{b^c}{(1-\frac{1}{x})^c(1-\frac{4}{x})^c} \\
&\le \frac{b^c}{(1-\frac{4}{x})^{2c}} \\
&\le \frac{b^c}{1-\frac{8c}{x}} \\
&\le b^c\Big(1+\frac{8c}{x}\Big).
\end{aligned} \tag{2.4.7}$$