1 H10 and Diophantine Set

Definition 1 (Hilbert 10th Problem)**.** Input $f \in \mathbb{Z}[X_1, ..., X_n]$. Does there exist $\underline{x} \in \mathbb{Z}^n$ such that $f(\underline{x}) = 0$?

Definition 2. A set $A \subseteq \mathbb{N}^m$ is diophantine if there is a polynomial $p \in \mathbb{Z}[A_1, \dots A_n, X_1, ..., X_n]$, such that $A = \{\underline{x} \in \mathbb{N} : \exists \underline{y}\ p(\underline{x}, \underline{y}) = 0\}$

Definition 3. A function $f : \mathbb{N}^m \to \mathbb{N}^n$ is diophantine if its graph is a Diophantine set, i.e. if

$$\{x_1, \dots, x_m, y \mid y = f(x_1, \dots, x_m)\}$$

is a diophantine set. Similarly define a diophantine relation on the natural numbers.

Theorem 1. *[Davis, Putnam, Robinson 1961; Matiyasevich 1970 [Mat93]] $A \subseteq \mathbb{N}^m$ is diophantine $\iff$ A is listable.*

Theorem 1 has the following consequence:

Corollary 1. *H10 is undecidable.*

In this note we give the idea of the proof of the fact that the exponential is diophantine, following [Dav73].

2 Examples of Diophantine Sets

2.1 Exponential Function

Is the function $h(n, k) = n^k$ diophantine?

Historically this is a very important question. It is positive answer of this problem by Matiyasevich that led to the negative answer of H10. Here we give the idea of the proof.

2.1.1 Pell's Equations

At the heart of the proof, we have the Pell equation:

$$x^2 - (a^2 - 1)y^2 = 1$$

Recall: the non-negative solutions to this equation is $\{x_n(a), y_n(a)\}_{n\in\mathbb{N}}$ given by

$$x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$$

Note that this is an analogue to the familiar formula $(\cos u) + (\sin u)i = e^{iu} = (\cos 1 + (\sin 1)i)^u$. x_n, y_n satisfy the following facts:

1. $x_0 = 1$, $y_0 = 0$; $x_1 = a$, $y_0 = 1$
2. $y_{m\pm1} = ay_m \pm x_m$, $x_{m\pm1} = ax_m \pm dy_m$
3. $x_{n+1} = 2ax_n - x_{n-1}$, $y_{n+1} = 2ay_n - y_{n-1}$

We will use this sequence to approximate the exponential, thanks to the following lemma:

Lemma 1. *For all $k, n \in \mathbb{N}$ we have*

$$x_k(a) - y_k(a)(a - n) \equiv n^k \pmod{2an - n^2 - 1}$$

Proof. Induction, using the properties mentioned above. □

The right hand side of the equation looks very good. In fact, it can be proven that given a, k, the function $f(k, a) = x_k(a)$ is diophantine. This gives us the idea to proceed.

The proof also required the following facts, whose proof are easy and not very interesting so we skip the details here.

Lemma 2. *Suppose x, y be a non-negative solution to $x^2 - (a^2 - 1)y^2 = 1$. Then for some n, $x = x_n, y = y_n$.*

Lemma 3. *If $y_n^2 \mid y_t$, then $y_n \mid t$.*

Lemma 4. $y_n(a) \equiv n \pmod{a-1}$.

Lemma 5. *If* $a \equiv b \pmod{c}$, *then for all* n, $x_n(a) \equiv x_n(b), y_n(a) \equiv y_j(b) \pmod{c}$.

Lemma 6. *For all* n, $x_{n+1}(a) > x_n(a) \geq a^n$

Lemma 7. $x_{2n \pm j} \equiv -x_j \pmod{x_n}$

Lemma 8. *If* $0 < i < n$ *and* $x_j \equiv x_i \pmod{x_n}$, *then* $j \equiv \pm i \pmod{4n}$

Lemma 9. *If* $a > y^k$, *then* $2ay - y^2 - 1 > y^k$

2.1.2 8 Equations

We will now show that the function $f(k, a) = x_k(a)$ is diophantine. Consider the following equations:

(1) $x^2 - (a^2 - 1)y^2 = 1$

(2) $u^2 - (a^2 - 1)v^2 = 1$

(3) $s^2 - (b^2 - 1)t^2 = 1$

(4) $v = ry^2$

(5) $b = 1 + 4py = a + qu$

(6) $s = x + cu$

(7) $t = k + 4(d - 1)y$

(8) $y = k + e - 1$

Claim 1. *For given* $a, x, k \in \mathbb{N}$ *and* $a > 1$, *this system of equations has a solution in the rest of the variables iff* $x = x_k(a)$.

Proof. We prove the $\implies$ direction.

The first three equations says that there exists $i, n, j \in \mathbb{N}$ such that

$$x = x_i(a), y = y_i(a), u = x_n(a), v = y_n(a), s = x_j(b), t = y_j(b)$$

The rest of the equations are there to force $i = k$.

(4) $\implies y \leq v$, therefore $i \leq n$.

(5) $\implies b \equiv a \pmod{u = x_n(a)}$. Due to Lemma 5 we get $x_j(b) \equiv x_j(a) \pmod{u = x_n(a)}$

(6) $\implies (s = x_j(b)) \equiv (x = x_i(a)) \pmod{u = x_n(a)}$. Using the previous line, we get

$$x_j(a) \equiv x_i(a) \pmod{u = x_n(a)}$$

Using Lemma 8, we get

$$j \equiv \pm i \pmod{4n} \qquad (\star)$$

Next, because of (4), $y_i(a)^2 \mid y_n(a)$, by Lemma 3 we get $y_i(a) \mid n$. This and $(\star)$ implies

$$j \equiv \pm i \pmod{4y_i(a)}$$

(5) $\implies b \equiv 1 \pmod{y = y_i(a)}$. So by Lemma 4, we get $(y_j(b) = t) \equiv j \pmod{4y_i(a)}$

But we already know by (7) that

$$(t = y_j(b)) \equiv k \pmod{4y_i(a)}$$

Therefore

$$j \equiv k \equiv \pm i \pmod{4y_i(a)}$$

But (8) $\implies (y = y_i(a)) \geq k$, and so if there is a positive solution for i, $k = i$. □

2.1.3 Rest of the proof

Based on what we have just seen, let us establish the fact that

Theorem 2. *$m = n^k$ is diophantine.*

Proof. Using Lemma 1 above, it would be very good if $m \equiv x_k(a) - y_k(a)(a-n) \pmod{2an - n^2 - 1}$.

We already know that $x_k(a)$ and $y_k(a)$ can already be described by 8 equations. We add to the 8 equations an additional 4:

(9) $(x - y(a-n) - m)^2 = (f-1)^2(2an - n^2 - 1)$[21]

(10) $m + g = 2an - n^2 - 1$

(11) $w = n + h = k + l$

(12) $a^2 - (w^2 - 1)(w-1)^2 z^2 = 1$

So now if (9) is satisfied, we have $m \equiv x_k(a) - y_k(a)(a-n) \pmod{2an - n^2 - 1}$.

Now, if we let a become large enough, we get $m = n^k$. Equation (12) provides a condition, which when satisfied, ensures a is large enough:

Claim 2. *$a > n^k$.*

Proof. Suppose a satisfies equation (11), then $a = x_j(w)$, $(w-1)z = y_j(w)$, for some j. By Lemma 4, we see that $(w-1)z = y_j(w) \equiv 0 \equiv j \pmod{w-1}$.

Therefore from Lemma 6, $a \geq w^j \geq w^{w-1} > n^k$ (from (11)).

Now, from Lemma 9, $n^k < 2an - n^2 - 1$. (10) gives $m < 2an - n^2 - 1$. Since m and n^k are congruent and both less than the modulus, they must be equal. □

This can all be done through 12 equation. When they are all satisfied, $m = n^k$ is guaranteed. Conversely, given $m = n^k$, we can construct Pell equations that satisfy the 12 equations and give rise to m and n. This then proves $m = n^k$ is diophantine. □

2.2 Binomial Coefficient

From the fact that exponential is diophantine, we can prove that $\binom{n}{k}$ is diophantine. We will break the proof down into several steps.

Definition 4. For any $\alpha \in \mathbb{R}$, let $\lfloor \alpha \rfloor$ be the integer such that

$$\lfloor \alpha \rfloor \leq \alpha < \lfloor \alpha \rfloor + 1$$

Claim 3. *For $w, x, y \in \mathbb{Z}$, $w = \lfloor x/y \rfloor$ is a diophantine relation.*

Proof. $w = \lfloor x/y \rfloor \iff w \leq x/y < w+1 \iff wy \leq x < wy + y$. □

Lemma 10. *For $k, n, u \in \mathbb{Z}$ such that $0 < k \leq n$ and $u > 2^n$,*

$$\lfloor (u+1)^n / u^k \rfloor = \sum_{i=k}^{n} \binom{n}{k} u^{i-k}$$

Proof. Note that $(u+1)^n/u^k = \sum_{i=0}^{n} \binom{n}{k} u^{i-k}$ can be split into an obviously integer part, and another part that can be proven to be less than 1 (by assumption on u):

$$\sum_{i=0}^{k-1} \binom{n}{k} u^{i-k} \leq u^{-1} \sum_{i=0}^{n} \binom{n}{k} = u^{-1} 2^n < 1$$

□

Note that the expression $w = \lfloor (u+1)^n / u^k \rfloor$ is also a diophantine relation, because we have already proven that the exponential is.

We have the following easy lemma:

Lemma 11. *For $u > 2^n$, $\lfloor (u+1)^n / u^k \rfloor \equiv \binom{n}{k} \pmod{u}$*

[21] The square is here, because f is supposed to be positive, and want to include the case where $(x - y(a-n) - m)$ is a negative multiple of $(2an - n^2 - 1)$.

Also note that $\binom{n}{k} < 2^n < u$, therefore we know that $\binom{n}{u}$ is the unique positive integer congruent to $\lfloor (u+1)^n/u^k \rfloor \pmod{u}$ and less than u.

$$z = \binom{n}{k} \iff (\exists u, v, w)(v = 2^n \wedge u > v \wedge w = \lfloor (u+1)^n/u^k \rfloor) \wedge z \equiv w \pmod{u} \wedge z < u$$

And this is a diophantine equation.

2.3 Factorial

We wish to show that for any $x \in \mathbb{N}$, $x!$ is diophantine. This is not hard thanks to the following lemma:

Lemma 12. *If $r \in \mathbb{N}$ satisfy $r > (2x)^{x+1}$,*

$$x! = \left\lfloor \frac{r^x}{\binom{r}{x}} \right\rfloor$$

Once we have this lemma, it is easy since we have already shown that $\lfloor a/b \rfloor$, exponential and $\binom{r}{x}$ are all diophantine.

Proof of Lemma 12.

$$\frac{r^x}{\binom{r}{x}} = x! \left\lfloor \frac{1}{(1-\frac{1}{r}) \cdots (1-\frac{x-1}{r})} \right\rfloor < x! \left(\frac{1}{(1-\frac{x}{r})^x} \right)$$

But then, by expanding Taylor series or otherwise, we get

$$\frac{1}{1-\frac{x}{r}} = 1 + \frac{x}{r} + (\frac{x}{r})^2 + \cdots < 1 + \frac{2x}{r};$$

$$(1 + \frac{2x}{r})^x = \sum_{j=0}^{x} \binom{x}{j} (\frac{2x}{r})^j < 1 + \frac{2x}{r} 2^x$$

.

Substituting we see

$$\frac{r^x}{\binom{r}{x}} < x! + \frac{2x}{r} x! 2^x < x! + \frac{2^{x+1} x^{x+1}}{r} < x! + 1$$

Therefore,

$$m = x! \iff \left\{ r > (2x)^{x+1} \wedge v = \binom{r}{x} \wedge mv \leq r^n < (m+1)v \right\}$$

But to express $r > (2n)^{n+1}$, we can use the following expression:

$$(\exists r, s, t)\left\{ s = 2x + 1 \wedge t = x + 1 \wedge r = s^t \right\}$$

□

References

[Dav73] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

[Mat93] Yuri V. Matiyasevich. *Hilbert's tenth problem.* MIT Press, Cambridge, MA, USA, 1993.