A talk invited by Liaoning Normal Univ. (Dec. 14, 2017)
and Nanjing Normal Univ. (Sept. 6, 2021)

Introduction to Lucas Sequences

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

Sept. 6, 2021

Abstract

Let A and B be integers. The Lucas sequences $u_n = u_n(A, B)$ $(n = 0, 1, 2, \ldots)$ and $v_n = v_0(A, B)$ $(n = 0, 1, 2, \ldots)$ are defined by

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots)$$

and

$$v_0 = 2,\ v_1 = A,\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

They are natural extensions of the Fibonacci numbers and the Lucas numbers. Lucas sequences play important roles in number theory and combinatorics. In this talk we introduce various properties of Lucas sequences and their applications. In particular, we will mention their elegant application to Hilbert's Tenth Problem on Diophantine equations.

Fibonacci numbers

In a book in 1202, Fibonacci considered the growth of an idealized (biologically unrealistic) rabbit population, assuming that: a newly born pair of rabbits, one male, one female, are put in a field; rabbits are able to mate at the age of one month so that at the end of its second month a female can produce another pair of rabbits; rabbits never die and a mating pair always produces one new pair (one male, one female) every month from the second month on. The puzzle that Fibonacci posed was: how many pairs will there be in one year?

Suppose that in the n-th month there are totally F_n pairs of rabbits. Then

$$F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots).$$

Note that

$$F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ F_7 = 13,$$
$$F_8 = 21,\ F_9 = 34,\ F_{10} = 55,\ F_{11} = 89,\ F_{12} = 144.$$

A combinatorial interpretation of Fibonacci numbers

Let $f(n)$ denote the number of binary sequences not containing two consecutive zeroes.

Clearly, $f(1) = 2$ (both 0 and 1 meet the purpose), and $f(2) = 3$ $(01, 10, 11$ meet the purpose).

Now let $a_1, \ldots, a_n \in \{0, 1\}$. Clearly $a_1 \ldots, a_n 1$ meets the purpose if and only if the sequence $a_1 \ldots, a_n$ meets the purpose. Also, the sequence $a_1 \ldots, a_n 0$ meets the purpose if and only if $a_n = 1$ and the sequence $a_1 \ldots a_{n-1}$ meets the purpose. Therefore

$$f(n+1) = f(n) + f(n-1).$$

Since $f(1) = F_3$, $f(2) = F_4$ and also $f(n+1) = f(n) + f(n-1)$ for $n = 1, 2, 3, \ldots$, we see that

$$f(n) = F_{n+2}.$$

Edouard Lucas

The name “*Fibonacci numbers* or *the Fibonacci sequence*” was first used by the French mathematician E. Lucas (1842-1891).

Lucas has several fundamental contributions to number theory.

Lucas’ Congruence. Let p be a prime, and let $a = \sum_{i=0}^{k} a_i p^i$ and $b = \sum_{i=0}^{k} b_i p^i$ with $a_i, b_i \in \{0, \ldots, p-1\}$. Then

$$\binom{a}{b} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \pmod{p}.$$

Lucas died in unusual circumstances. At the banquet of an annual congress, a waiter dropped some crockery and a piece of broken plate cut Lucas on the cheek. He died a few days later of a severe skin inflammation probably caused by septicemia. He was only 49.

Lucas sequences

Let A and B be given numbers. For $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ we define $u_n = u_n(A, B)$ and $v_n = v_n(A, B)$ as follows:

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots);$$
$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

The sequence $\{u_n\}_{n\in\mathbb{N}}$ and its companion $\{v_n\}_{n\in\mathbb{N}}$ are called *Lucas sequences*.

In 1876 E. Lucas introduced such sequences in the case $A, B \in \mathbb{Z}$, and studied them systematically. Lucas sequences play important roles in number theory.

Special cases

By induction on $n \in \mathbb{N}$ we find that

$$u_n(2,1) = n,\ v_n(2,1) = 2;\ u_n(3,2) = 2^n - 1,\ v_n(3,2) = \frac{2^n + 1}{3}.$$

Those $F_n = u_n(1,-1)$ and $L_n = v_n(1,-1)$ are called *Fibonacci numbers* and *Lucas numbers* respectively. The *Pell sequence* $\{P_n\}_{n\in\mathbb{N}}$ is given by $P_n = u_n(2,-1)$, so

$$P_0 = 0,\ P_1 = 1,\ P_{n+1} = 2P_n + P_{n-1}\ (n = 1,2,3,\ldots).$$

The companion of the Pell sequence is $\{Q_n\}_{n\in\mathbb{N}}$ where $Q_n = v_n(2,-1)$. We also let $S_n = u_n(4,1)$ and $T_n = v_n(4,1)$; thus

$$S_0 = 0,\ S_1 = 1,\ \text{and } S_{n+1} = 4S_n - S_{n-1}\ (n = 1,2,3,\ldots);$$
$$T_0 = 2,\ T_1 = 4,\ T_{n+1} = 4T_n - T_{n-1}\ (n = 1,2,3,\ldots).$$

Binet Formulae

The equation $x^2 = Ax - B$ is called the characteristic equation of the Lucas sequences $\{u_n(A,B)\}_{n\in\mathbb{N}}$ and $\{v_n(A,B)\}_{n\in\mathbb{N}}$.
$\Delta = A^2 - 4B$ is the discriminant, and the two roots are

$$\alpha = \frac{A+\sqrt{\Delta}}{2} \text{ and } \beta = \frac{A-\sqrt{\Delta}}{2}.$$

Property 1 (Binet, 1843) For any $n = 0, 1, 2, \ldots$ we have

$$u_n = \sum_{0\leqslant k<n} \alpha^k \beta^{n-1-k} \text{ and } v_n = \alpha^n + \beta^n.$$

As $A = \alpha + \beta$ and $B = \alpha\beta$, we can prove the formulae by induction on n.

If $\Delta = 0$, then $\alpha = \beta = A/2$, hence

$$u_n = \sum_{0\leqslant k<n} \alpha^{n-1} = n\left(\frac{A}{2}\right)^{n-1} \text{ and } v_n = 2\alpha^n = 2\left(\frac{A}{2}\right)^n.$$

Explicit Formulae

We can express u_n and v_n in terms of n, A and Δ. In fact,

$$\begin{aligned}\sqrt{\Delta}u_n =&(\alpha-\beta)u_n = \alpha^n - \beta^n = \left(\frac{A+\sqrt{\Delta}}{2}\right)^n - \left(\frac{A-\sqrt{\Delta}}{2}\right)^n \\ =&\frac{\sqrt{\Delta}}{2^{n-1}} \sum_{\substack{k=0 \\ 2\nmid k}}^{n} \binom{n}{k} A^{n-k}\Delta^{(k-1)/2}\end{aligned}$$

and thus

$$2^{n-1}u_n = \sum_{k=0}^{\lfloor (n-1)/2\rfloor} \binom{n}{2k+1} A^{n-1-2k}\Delta^k$$

(which also holds when $\Delta = 0$). Similarly,

$$\begin{aligned}v_n =&\alpha^n + \beta^n = \left(\frac{A+\sqrt{\Delta}}{2}\right)^n + \left(\frac{A-\sqrt{\Delta}}{2}\right)^n \\ =&\frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor n/2\rfloor} \binom{n}{2k} A^{n-2k}\Delta^k.\end{aligned}$$

Special cases

For the Fibonacci sequence $\{F_n\}_{n\in\mathbb{N}}$ and its companion $\{L_n\}_{n\in\mathbb{N}}$, $\Delta = 1^2 - 4(-1) = 5$ and so

$$\sqrt{5}F_n = \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n, \ L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

For the Pell sequence $\{P_n\}_{n\in\mathbb{N}}$ and its companion $\{Q_n\}_{n\in\mathbb{N}}$, $\Delta = 2^2 - 4(-1) = 8$ and so

$$2\sqrt{2}P_n = (1+\sqrt{2})^n - (1-\sqrt{2})^n, \ Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n.$$

For the sequence $\{S_n\}_{n\in\mathbb{N}}$ and its companion $\{T_n\}_{n\in\mathbb{N}}$, $\Delta = 4^2 - 4\cdot 1 = 12$ and so

$$S_n = \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right), \ T_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n.$$

On $((A+\sqrt{A^2-4B})/2)^n$

Let $A, B \in \mathbb{Z}$ with $\Delta = A^2 - 4B$. For $n \in \mathbb{N}$, as

$$\sqrt{\Delta} u_n(A,B) = \left(\frac{A+\sqrt{\Delta}}{2}\right)^n - \left(\frac{A-\sqrt{\Delta}}{2}\right)^n,$$

$$v_n(A,B) = \left(\frac{A+\sqrt{\Delta}}{2}\right)^n + \left(\frac{A-\sqrt{\Delta}}{2}\right)^n,$$

we have

$$\left(\frac{A\pm\sqrt{\Delta}}{2}\right)^n = \frac{v_n(A,B) \pm u_n(A,B)\sqrt{\Delta}}{2}.$$

In particular,

$$\left(\frac{1\pm\sqrt{5}}{2}\right)^n = \frac{L_n \pm F_n\sqrt{5}}{2},$$

$$(1\pm\sqrt{2})^n = \frac{Q_n}{2} \pm P_n\sqrt{2}, \quad (2\pm\sqrt{3})^n = \frac{T_n}{2} \pm S_n\sqrt{3}.$$

Relations between u_n and v_n

Property 2. For $n \in \mathbb{N}$ we have

$$v_n = 2u_{n+1} - Au_n,\ \Delta u_n = 2v_{n+1} - Av_n,\ v_n^2 - \Delta u_n^2 = 4B^n.$$

This can be easily proved since

$$A = \alpha + \beta,\ \sqrt{\Delta} u_n = \alpha^n - \beta^n,\ v_n = \alpha^n + \beta^n,$$

where

$$\Delta = A^2 - 4B,\ \alpha = \frac{A + \sqrt{\Delta}}{2} \text{ and } \beta = \frac{A - \sqrt{\Delta}}{2}.$$

In particular,

$$L_n = 2F_{n+1} - F_n,\ 5F_n = 2L_{n+1} - L_n,\ L_n^2 - 5F_n^2 = 4(-1)^n.$$

Neighbouring formulae

Property 3 (Neighbouring formulae). For any $n \in \mathbb{N}$ we have

$$u_{n+1}^2 - Au_{n+1}u_n + Bu_n^2 = B^n,\ v_{n+1}^2 - Av_{n+1}v_n + Bv_n^2 = -\Delta B^n.$$

In other words, if $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ then

$$u_n^2 - u_{n-1}u_{n+1} = B^{n-1} \text{ and } v_n^2 - v_{n-1}v_{n+1} = -\Delta B^{n-1}.$$

Proof. By Property 2,

$$4B^n = v_n^2 - \Delta u_n^2 = (2u_{n+1} - Au_n)^2 - \Delta u_n^2$$

and

$$4\Delta B^n = \Delta v_n^2 - (\Delta u_n)^2 = \Delta v_n^2 - (2v_{n+1} - 4Av_n)^2.$$

So the desired results follow.

Example.

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n,\ L_{n+1}^2 - L_{n+1}L_n - L_n^2 = 5(-1)^{n-1}.$$

Addition formulae

Property 4 (Addition Formulae). For any $m, n \in \mathbb{N}$ we have

$$u_{m+n} = \frac{u_m v_n + u_n v_m}{2}$$

and

$$v_{m+n} = \frac{v_m v_n + \Delta u_m u_n}{2}.$$

Property 5 (Double Formulae). For each $n \in \mathbb{N}$ we have

$$u_{2n} = u_n v_n, \; v_{2n} = v_n^2 - 2B^n = \frac{v_n^2 + \Delta u_n^2}{2} = \Delta u_n^2 + 2B^n,$$

$$u_{2n+1} = u_{n+1}^2 - Bu_n^2, \; v_{2n+1} = v_n v_{n+1} - AB^n.$$

Multiplication Formulae

Property 6 (Multiplication Formulae). For any $k, n \in \mathbb{N}$ we have

$$u_{kn} = u_k \cdot u_n(v_k, B^k) \text{ and } v_{kn} = v_n(v_k, B^k).$$

Proof. Let $A' = v_k$ and $B' = B^k$. Then $\Delta' = v_k^2 - 4B^k = \Delta u_k^2$,

$$\alpha' = \frac{v_k + \sqrt{\Delta} u_k}{2}, \quad \beta' = \frac{v_k - \sqrt{\Delta} u_k}{2}.$$

Hence

$$\begin{aligned}(\alpha')^n + (\beta')^n &= \left(\frac{v_k + \sqrt{\Delta} u_k}{2}\right)^n + \left(\frac{v_k - \sqrt{\Delta} u_k}{2}\right)^n \\ &= \left(\frac{A + \sqrt{\Delta}}{2}\right)^{kn} + \left(\frac{A - \sqrt{\Delta}}{2}\right)^{kn} = v_{kn}.\end{aligned}$$

That $u_{kn} = u_k \cdot u_n(v_k, B^k)$ can be proved similarly.

Expansions in terms of A and B

Property 7 (Expansions in terms of A and B). For any $n \in \mathbb{Z}^+$ we have

$$u_n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} A^{n-1-2k}(-B)^k,$$

$$v_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} A^{n-2k}(-B)^k.$$

Proof. Observe that

$$\begin{aligned}\sum_{m=1}^{\infty} u_m x^{m-1} &= \sum_{m=1}^{\infty} \sum_{k=0}^{m-1} \alpha^k \beta^{m-1-k} x^{m-1} \\ &= \sum_{m=1}^{\infty} \sum_{k=0}^{m-1} (\alpha x)^k (\beta x)^{m-1-k} = \sum_{k=0}^{\infty} (\alpha x)^k \sum_{j=0}^{\infty} (\beta x)^j \\ &= \frac{1}{1-\alpha x} \cdot \frac{1}{1-\beta x} = \frac{1}{1-Ax+Bx^2}.\end{aligned}$$

Expansions in terms of A and B (continued)

Let $[x^m]f(x)$ denote the coefficient of x^m in the power series for $f(x)$. Then

$$\begin{aligned}
u_n =&[x^{n-1}]\sum_{m=1}^{\infty} u_m x^{m-1} = [x^{n-1}]\frac{1}{1-Ax+Bx^2} \\
=&[x^{n-1}]\frac{1-(x(A-Bx))^n}{1-x(A-Bx)} = [x^{n-1}]\sum_{k=0}^{n-1} x^k (A-Bx)^k \\
=&[x^{n-1}]\sum_{k=0}^{n-1} x^{n-1-k}(A-Bx)^{n-1-k} \\
=&\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k}(-B)^k A^{n-1-k-k} \\
=&\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} A^{n-1-2k}(-B)^k.
\end{aligned}$$

Expansions in terms of A and B (continued)

$$\begin{aligned}
v_n =& 2u_{n+1} - Au_n \\
=& 2\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} A^{n-2k}(-B)^k \\
& - A \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} A^{n-1-2k}(-B)^k \\
=& \sum_{k=0}^{\lfloor n/2 \rfloor} \left(2\binom{n-k}{k} - \binom{n-1-k}{k} \right) A^{n-2k}(-B)^k \\
=& \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} A^{n-2k}(-B)^k.
\end{aligned}$$

Corollary. For any $n \in \mathbb{Z}^+$ we have

$$F_n = \sum_{k \in \mathbb{N}} \binom{n-1-k}{k} \quad \text{and} \quad L_n = \sum_{0 \leqslant k \leqslant n/2} \frac{n}{n-k} \binom{n-k}{k}.$$

On linear index

Property 8 (On linear index) (Z.-W. Sun [Sci. China Ser. A 35(1992)]). Suppose that

$$w_{n+1} = Aw_n - Bw_{n-1} \text{ for } n = 1, 2, 3, \ldots .$$

Then, for any $k \in \mathbb{Z}^+$ and $l, n \in \mathbb{N}$ we have

$$w_{kn+l} = \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j w_{l+j},$$

in particular

$$w_{2n+l} = \sum_{j=0}^{n} \binom{n}{j} (-B)^{n-j} A^j w_{l+j}.$$

Corollary. For any $n \in \mathbb{N}$ we have

$$F_{2n} = \sum_{j=0}^{n} \binom{n}{j} F_j \quad \text{and} \quad F_{2n+1} = \sum_{j=0}^{n} \binom{n}{j} F_{j+1}.$$

On linear index (continued)

We prove the identity by induction on n. The case $n = 0$ is trivial.

Now assume that the identity for n is valid. Then

$$\begin{aligned}
w_{k(n+1)+l} =& w_{kn+(k+l)} = \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j w_{k+l+j} \\
=& \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j (u_k w_{l+j+1} - Bu_{k-1} w_{l+j}) \\
=& u_k^{n+1} w_{l+n+1} + \sum_{j=1}^{n} \binom{n}{j-1} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j} \\
&+ \sum_{j=1}^{n} \binom{n}{j} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j} + (-Bu_{k-1})^{n+1} w_l \\
=& \sum_{j=0}^{n+1} \binom{n+1}{j} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j}.
\end{aligned}$$

Lucas' Theorem

Property 9 (E. Lucas) Let $A, B \in \mathbb{Z}$ with $(A, B) = 1$. Then

$$(u_m, u_n) = |u_{(m,n)}| \quad \text{for all } m, n \in \mathbb{N}.$$

Proof. By induction, $u_{n+1} \equiv A^n \pmod{B}$. As $(A, B) = 1$, we have $(u_{n+1}, B) = 1$. Since $u_{n+1}^2 - Au_{n+1}u_n + Bu_n^2 = B^n$ by Property 3, $(u_n, u_{n+1}) \mid B^n$ and hence $(u_n, u_{n+1}) \mid (u_{n+1}, B^n) = 1$.

By Property 8, for any $n \in \mathbb{Z}^+$ and $q, r \in \mathbb{N}$ we have

$$\begin{aligned} u_{nq+r} =& \sum_{j=0}^{q} \binom{q}{j} (-Bu_{n-1})^{q-j} u_n^j u_{r+j} \\ \equiv& (-Bu_{n-1})^q u_r = (u_{n+1} - Au_n)^q u_r \equiv u_{n+1}^q u_r \pmod{u_n} \end{aligned}$$

and hence

$$(u_{nq+r}, u_n) = (u_n, u_r).$$

Lucas' Theorem (continued)

Clearly, $(u_m, u_0) = (u_m, 0) = |u_m| = |u_{(m,0)}|$.

Now let $r_0 = m$ and $r_1 = n \in \mathbb{Z}^+$. Write $r_{i-1} = r_i q_i + r_{i+1}$ for $i = 1, \dots, k$ with $r_1 > r_2 > \dots > r_k > r_{k+1} = 0$. For each $i = 1, \dots, k$,

$$(u_{r_{i-1}}, u_{r_i}) = (u_{q_i r_i + r_{i+1}}, u_{r_i}) = (u_{r_i}, u_{r_{i+1}}).$$

Therefore,

$$\begin{aligned}(u_m, u_n) =& (u_{r_0}, u_{r_1}) = (u_{r_1}, u_{r_2}) = \dots \\ =& (u_{r_k}, u_{r_{k+1}}) = (u_{(m,n)}, u_0) = |u_{(m,n)}|.\end{aligned}$$

Remark. For $m, n \in \mathbb{Z}^+$, we can prove that

$$(v_m, v_n) = \begin{cases} |v_{(m,n)}| & \text{if } \mathrm{ord}_2(m) = \mathrm{ord}_2(n), \\ (2, v_{(m,n)}) & \text{otherwise.} \end{cases}$$

On positivity of u_n and v_n

Property 10 (Z.-W. Sun [PhD thesis, 1992]).

$$\begin{aligned} & u_n \geqslant 0 \text{ for all } n \in \mathbb{N} \\ \iff & v_n \geqslant 0 \text{ for all } n \in \mathbb{N} \\ \iff & A \geqslant 0 \text{ and } \Delta = A^2 - 4B \geqslant 0. \end{aligned}$$

Proof. If $A \geqslant 0$ and $\Delta \geqslant 0$, then $u_n \geqslant 0$ and $v_n \geqslant 0$ by the explicit formulae in terms of A and Δ.

Suppose that $u_n \geqslant 0$ for all $n \in \mathbb{N}$. Then $A = u_2 \geqslant 0$. If $\Delta < 0$, then $u_{n+1}^2 - u_n u_{n+2} = B^n > 0$ and the decreasing sequence $(u_{n+1}/u_n)_{n \geqslant 1}$ has a real number limit θ. Since

$$\frac{u_{n+2}}{u_{n+1}} = \frac{Au_{n+1} - Bu_n}{u_{n+1}} = A - \frac{B}{u_{n+1}/u_n} \ (n = 1, 2, 3, \ldots),$$

we see that $\theta^2 - A\theta + B = 0$ and thus $\Delta \geqslant 0$. Similarly, if $v_n \geqslant 0$ for all $n \in \mathbb{N}$ then $A = v_0 \geqslant 0$ and $\Delta \geqslant 0$.

Periodicity of u_n and v_n modulo m

Property 11 (Periodicity of u_n and v_n modulo m). Let $m \in \mathbb{Z}^+$ with $(B, m) = 1$. Then there is a positive integer λ such that

$$u_{n+\lambda} \equiv u_n \pmod{m} \quad \text{for all } n \in \mathbb{N}$$

and also

$$v_{n+\lambda} \equiv v_n \pmod{m} \quad \text{for all } n \in \mathbb{N}.$$

Proof. Consider the $m^2 + 1$ ordered pairs

$$\langle u_i, u_{i+1} \rangle \ (i = 0, \ldots, m^2).$$

By the Pigeon-hole Principle, two of them are congruent modulo m. Choose the least $\lambda \leqslant m^2$ such that

$$\langle u_\lambda, u_{\lambda+1} \rangle \equiv \langle u_j, u_{j+1} \rangle \pmod{m}$$

for some $0 \leqslant j < \lambda$. Since

$$-Bu_{j-1} = u_{j+1} - Au_j \equiv u_{\lambda+1} - Au_\lambda = -Bu_{\lambda-1} \pmod{m}$$

and $(B, m) = 1$, we get $u_{j-1} \equiv u_{\lambda-1} \pmod{m}$. Continuing this process, we finally obtain $\langle u_{\lambda-j}, u_{\lambda-j+1} \rangle \equiv \langle u_0, u_1 \rangle \pmod{m}$.

Periodicity of u_n and v_n modulo m (continued)

By the choice of λ, we must have $j = 0$ and thus

$$\langle u_\lambda, u_{\lambda+1} \rangle \equiv \langle u_0, u_1 \rangle \pmod{m}.$$

It follows that $u_{n+\lambda} \equiv u_n \pmod{m}$ for all $n = 0, 1, 2, \ldots$.

For any $n \in \mathbb{N}$, we also have

$$v_{n+\lambda} = 2u_{n+\lambda+1} - Au_{n+\lambda} \equiv 2u_{n+1} - Au_n = v_n \pmod{m}.$$

This completes the proof.

Legendre symbols

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $(\frac{a}{p})$ is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some } x \in \mathbb{Z}, \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for no } x \in \mathbb{Z}. \end{cases}$$

It is well known that $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ for any $a, b \in \mathbb{Z}$. Also,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv -1 \pmod{4}; \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

The Law of Quadratic Reciprocity: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Lucas sequences modulo primes

Property 12. Let $A, B \in \mathbb{Z}$ with $\Delta = A^2 - 4B$, and let p be an odd prime.

(i) $u_p \equiv (\frac{\Delta}{p}) \pmod{p}$ and $v_p \equiv A \pmod{p}$.

(ii) If $p \nmid B$, then $p \mid u_{p-(\frac{\Delta}{p})}$.

Proof. Note that $p \mid \binom{p}{j}$ for all $j = 1, \ldots, p-1$. Thus

$$\begin{aligned} u_p \equiv 2^{p-1} u_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} A^{p-1-2k} \Delta^k \\ \equiv \Delta^{(p-1)/2} \equiv \left(\frac{\Delta}{p}\right) \pmod{p} \end{aligned}$$

and

$$\begin{aligned} v_p \equiv 2^{p-1} v_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} A^{p-2k} \Delta^k \\ \equiv A^p \equiv A \pmod{p}. \end{aligned}$$

Lucas sequences modulo primes

Now we prove $p \mid u_{p-(\frac{\Delta}{p})}$ under the condition $p \nmid B$.

If $p \mid \Delta$, then $u_{p-(\frac{\Delta}{p})} = u_p \equiv \left(\frac{\Delta}{p}\right) = 0 \pmod{p}$.

If $(\frac{\Delta}{p}) = -1$, then

$$2u_{p+1} = Au_p + v_p \equiv A\left(\frac{\Delta}{p}\right) + A = 0 \pmod{p}$$

and hence $u_{p-(\frac{\Delta}{p})} = u_{p+1} \equiv 0 \pmod{p}$.

In the case $(\frac{\Delta}{p}) = 1$, we have

$$Bu_{p-1} = Au_p - u_{p+1} = \frac{Au_p - v_p}{2} \equiv \frac{A}{2}(u_p - 1) \equiv 0 \pmod{p}$$

and hence $u_{p-(\frac{\Delta}{p})} = u_{p-1} \equiv 0 \pmod{p}$ since $p \nmid B$.

Wall-Sun-Sun primes

In 1960 D. D. Wall [Amer. Math. Monthly] investigated Fibonacci numbers modulo m. For $d \in \mathbb{Z}^+$ let $n(d)$ be the least $n \in \mathbb{Z}^+$ such that $d \mid F_n$. Wall asked whether $n(p) \neq n(p^2)$ for any odd prime p.

Let p be an odd prime. Then $F_{p-(\frac{p}{5})} = F_{p-(\frac{5}{p})} \equiv 0 \pmod{p}$.
Z.-H. Sun and Z.-W. Sun [Acta Arith. 60(1992)] proved that

$$\begin{aligned} n(p) \neq n(p^2) &\iff p^2 \nmid F_{p-(\frac{p}{5})} \\ &\implies x^p + y^p = z^p \text{ for no } x, y, z \in \mathbb{Z} \text{ with } p \nmid xyz. \end{aligned}$$

An odd prime p with $p^2 \mid F_{p-(\frac{p}{5})}$ is called a *Wall-Sun-Sun prime*. There are no known Wall-Sun-Sun primes though heuristic arguments suggest that there should be infinitely many Wall-Sun-Sun primes.

Chebyshev polynomials

The first kind of Chebyshev polynomials $T_n(x)$ ($n \in \mathbb{N}$) and the second kind of Chebyshev polynomials $U_n(x)$ ($n \in \mathbb{N}$) are given by

$$\cos n\theta = T_n(\cos\theta) \text{ and } \sin((n+1)\theta) = \sin\theta \cdot U_n(\cos\theta).$$

Clearly,

$$T_0(x) = 1,\ T_1(x) = x,\ T_2(x) = 2x^2 - 1,$$
$$U_0(x) = 1,\ U_1(x) = 2x,\ U_2(x) = 4x^2 - 1.$$

As

$$\cos(n\theta+\theta) = \cos\theta\cos n\theta - \sin\theta\sin n\theta = 2\cos\theta\cos n\theta - \cos(n\theta-\theta)$$

and

$$\sin(n\theta+\theta) = \cos\theta\sin n\theta + \sin\theta\cos n\theta = 2\cos\theta\sin n\theta - \sin(n\theta-\theta),$$

we have

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \text{ and } U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x).$$

Chebyshev polynomials (continued)

As

$$2T_0(x) = 2,\ 2T_1(x) = 2x,\ T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)\ (n = 1, 2, \ldots),$$

and

$$U_0(x) = 1,\ U_1(x) = 2x,\ U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)\ (n = 1, 2, \ldots),$$

we see that

$$2T_n(x) = v_n(2x, 1) \text{ and } U_n(x) = u_{n+1}(2x, 1).$$

Thus, for any $n \in \mathbb{Z}^+$, by Property 7 we have

$$T_n(x) = \frac{1}{2} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} (2x)^{n-2k} (-1)^k$$

and

$$U_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} (2x)^{n-2k} (-1)^k.$$

Pell's equation

Let $d \in \mathbb{Z}^+ \setminus \Box$. It is well-known that the Pell equation

$$y^2 - dx^2 = 1$$

has infinitely many integral solutions. (Note that $x = 0$ and $y = \pm 1$ are trivial solutions.) Moreover,

$$\{y + \sqrt{d}x : \ x, y \in \mathbb{Z} \text{ and } y^2 - dx^2 = 1\}$$

is a multiplicative cyclic group.

For any integer $A \geqslant 2$, the solutions of the Pell equation

$$y^2 - (A^2 - 1)x^2 = 1 \ \ (x, y \in \mathbb{N})$$

are given by $x = u_n(2A, 1)$ and $y = v_n(2A, 1)/2$ with $n \in \mathbb{N}$. J. Robinson and his followers wrote $u_n(2A, 1)$ and $v_n(2A, 1)$ as $\psi_n(A)$ and $\chi_n(A)$ respectively.

To unify Matiyasevich's use of $F_{2n} = u_n(3, 1)$ and Robinson's use of $\psi_n(A) = u_n(2A, 1)$, we deal with Lucas sequences $(u_n(A, 1))_{n \geqslant 0}$.

On $u_n(A,1)$ with $n \in \mathbb{Z}$

We extend the sequences $u_n = u_n(A,1)$ and $v_n = v_n(A,1)$ to integer indices by letting

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n-1} + u_{n+1} = Au_n \text{ for all } n \in \mathbb{Z},$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n-1} + v_{n+1} = Av_n \text{ for all } n \in \mathbb{Z}.$$

It is easy to see that

$$u_{-n}(A,1) = -u_n(A,1) = (-1)^n u_n(-A,1)$$

and $v_{-n}(A,1) = v_n(A,1) = (-1)^n v_n(-A,1)$ for all $n \in \mathbb{Z}$.

Lemma. Let $A, X \in \mathbb{Z}$. Then

$$(A^2-4)X^2+4 \in \Box \iff X = u_m(A,1) \text{ for some } m \in \mathbb{Z}.$$

Remark. For $n \in \mathbb{N}$ and $A \geqslant 2$, it is easy to show that

$$(A-1)^n \leqslant u_{n+1}(A,1) \leqslant A^n.$$

Hilbert's Tenth Problem

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. He formulated his tenth problem as follows:

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

In modern language, Hilbert's Tenth Problem (HTP) asked for an effective algorithm to test whether an arbitrary polynomial equation

$$P(z_1, \ldots, z_n) = 0$$

(with integer coefficients) has solutions over the ring $\mathbb{Z}$ of the integers.

However, at that time the exact meaning of algorithm was not known.

Two key steps to solve HTP

Based on the above theorem, M. Davis, H. Putnam and J. Robinson [Ann. of Math. 1961] successfully showed that any r.e. set is exponential Diophantine, that is, any r.e. set A has the exponential Diophantine representation

$$a \in A \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a, x_1, \ldots, x_n, 2^{x_1}, \ldots, 2^{x_n}) = 0],$$

where P is a polynomial with integer coefficients.

Recall that the Fibonacci sequence $(F_n)_{n \geqslant 0}$ defined by

$$F_0 = 0,\ F_1 = 1,\ \text{ and } F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots)$$

increases exponentially. In 1970 Yu. Matiyasevich took the last step to show ingeniously that the relation $y = F_{2x}$ (with $x, y \in \mathbb{N}$) is Diophantine! It follows that the exponential relation $a = b^c$ (with $a, b, c \in \mathbb{N}$, $b > 1$ and $c > 0$) is Diophantine, i.e. there exists a polynomial $P(a, b, c, x_1, \ldots, x_n)$ with integer coefficients such that

$$a = b^c \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 [P(a, b, c, x_1, \ldots, x_n) = 0].$$

A key lemma

The following lemma is an extension of a lemma of Yu. Matiyasevich (1970).

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B \in \mathbb{Z}$ with $(A, B) = 1$, and let $k, m \in \mathbb{N}$.

(i) $ku_k \mid m \implies u_k^2 \mid u_m$.

(ii) Suppose that $A \neq 0$, $A^2 \geqslant 4B$, and $|A| \neq 1$ or $(k-2)B \neq 0$. Then $u_k^2 \mid u_m \Rightarrow ku_k \mid m$.

Diophantine representation of $C = u_B(A, 1)$ with unknowns arbitrarily large

Matiyasevi c and Robinson (1975) showed that for $A > 1$ and $B, C > 0$ there is a Diophantine representation of $C = u_B(2A, 1)$ only involving three natural number variables.

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $A > 1$ and $B \geqslant 0$. Then

$$C = u_B(A, 1) \iff C \geqslant B \wedge \exists x > 0 \exists y > 0 (DFI \in \square)$$
$$\iff \exists x, y, z \geqslant 0 [DFI(C - B + 1)^2 = (z - DFI(C - B + 1))^2],$$

where

$$D = (A^2 - 4)C^2 + 4,\ E = C^2 Dx,\ F = 4(A^2 - 4)E^2 + 1,$$
$$G = 1 + CDF - 2(A + 2)(A - 2)^2 E^2,\ H = C + BF + (2y - 1)CF,$$
$$I = (G^2 - 1)H^2 + 1.$$

Moreover, if $C = u_B(A, 1)$ with $B > 0$, then for any $Z \in \mathbb{Z}^+$ there are integers $x \geqslant Z$ and $y \geqslant Z$ with $DFI \in \square$.

Diophantine representation of $C = u_B(A,1)$ with integer unknowns

Clearly $C \geqslant B \iff \exists x \geqslant 0 (C = B + x)$. However, if we use integer variables, we need three variables:

$$C \geqslant B \iff \exists x \exists y \exists z [C = B + x^2 + y^2 + z^2 + z].$$

Thus, to save the number of integer variables involved, we should try to avoid inequalities.

Note that

$$u_B(A,1) \equiv u_B(2,1) = B \pmod{A-2}.$$

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $1 < |B| < |A|/2 - 1$. Then

$$C = u_B(A,1) \iff (A - 2 \mid C - B) \wedge \exists x \neq 0 \exists y (DFI \in \square),$$

where D, F, I are defined as before.

A lemma

Lemma. Let $A, V \in \mathbb{Z}$. For any $B \in \mathbb{Z}^+$ we have

$$V^{B-1}u_B(A,1) \equiv \sum_{r=0}^{B-1} V^{2(B-1-r)} \pmod{AV - V^2 - 1}.$$

Proof. We write u_n for $u_n(A,1)$, and use induction on B.
The result holds for $B = 1, 2$ since

$V^0u_0 = 1 = V^{2(1-1-0)}$ and $Vu_2 = VA \equiv 1+V^2 \pmod{AV-V^2-1}$.

Now let $B > 2$ and assume the desired result for smaller B. Then

$$\begin{aligned} V^{B-1}u_B =& V^{B-1}(Au_{B-1} - u_{B-2}) = AV(V^{B-2}u_{B-1}) - V^2(V^{B-3}u_{B-2}) \\ \equiv& AV\sum_{r=0}^{B-2} V^{2(B-2-r)} - V^2\sum_{r=0}^{B-3} V^{2(B-3-r)} \\ \equiv& (V^2+1)\sum_{r=0}^{B-2} V^{2(B-2-r)} - \sum_{r=0}^{B-3} V^{2(B-2-r)} = \sum_{r=0}^{B-1} V^{2(B-1-r)} \\ & \pmod{AV - V^2 - 1}. \end{aligned}$$

Diophantine representation of $W = V^B$ over $\mathbb{N}$

Let $A, B, V \in \mathbb{Z}$ with $B \geqslant 0$. By the above,

$$(V^2 - 1)V^{B-1}u_B(A, 1) \equiv (V^{2B} - 1) \pmod{AV - V^2 - 1}$$

and hence

$$(V^2 - 1)V^B u_B(A, 1) \equiv V((V^B)^2 - 1) \pmod{AV - V^2 - 1}.$$

J. Robinson showed that $W = V^B$ (with $V > 1$ and $B, W > 0$) if and only if there is an integer $A > \max\{V^{3B}, W^3\}$ such that

$$(V^2 - 1)W\, u_B(2A, 1) \equiv V(W^2 - 1) \pmod{2AV - V^2 - 1}.$$

Another lemma

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $mx > 0$ and

$$Q(m,x,y) = 4m(mx+2)x^3y^2 + 1.$$

If $Q(m,x,y) \in \square$, then $y = 0$ or $|y| > |x|^{|x|}$.

Proof. Suppose that $y \neq 0$ and $Q(m,x,y) \in \square$. As

$$((2mx+2)^2 - 4)(2xy)^2 + 4 = 4Q(m,x,y) \in \square,$$

for some $n \in \mathbb{N}$ we have $0 < |2xy| = u_n(2mx+2,1)$ and

$$0 \equiv u_n(2,1) = n \pmod{2x}.$$

Hence $n \geqslant 2|x|$. If $|x| = 1$ then

$$2|y| = u_n(2mx+2,1) \geqslant u_2(2mx+2,1) = 2mx+2$$

and hence $|y| > |x|^{|x|} = 1$. If $|x| \geqslant 2$, then

$$2|xy| = u_n(2mx+2,1) \geqslant (2mx+1)^{n-1} > (2|x|)^{|x|+1} \geqslant 2|x|^{|x|+1}$$

and hence $|y| > |x|^{|x|}$.

Diophantine representation of $W = V^B$ with integer unknowns

Theorem (Sun [Sci. China Ser. A 35(1992)]). Let B, V, W be integers with $B > 0$ and $|V| > 1$. Then $W = V^B$ if there are $A, C \in \mathbb{Z}$ for which $|A| \geqslant \max\{V^{4B}, W^4\}$, $C = u_B(A, 1)$ and

$$(V^2 - 1)WC \equiv V(W^2 - 1) \pmod{AV - V^2 - 1}.$$

Proof. Since

$$\begin{aligned} V^B(W^2 - 1) \equiv& V^{B-1}(V^2 - 1)W\, u_B(A, 1) \\ \equiv& W(V^{2B} - 1) \pmod{AV - V^2 - 1}, \end{aligned}$$

we have

$$(V^B W + 1)(W - V^B) \equiv 0 \pmod{AV - V^2 - 1}.$$

Continue the proof

As $|A|^{1/4} \geqslant |V|^B \geqslant 2$ and

$$1 + |A|^{1/4} + |A|^{1/2} \leqslant |A|^{3/4} - 1 < |A|^{3/4},$$

we have

$$\begin{aligned} |(V^B W + 1)(W - V^B)| \leqslant & 2|A|^{1/4}(1 + |A|^{1/4+1/4}) \\ < & 2|A|^{1/4}(|A|^{3/4} - |A|^{1/4}) = 2|A| - 2|A|^{1/2} \\ \leqslant & |V||A| - 2V^2 \leqslant |AV| - (V^2 + 1) \\ \leqslant & |AV - V^2 - 1| \end{aligned}$$

and hence $(V^B W + 1)(W - V^B) = 0$.

Obviously $W \neq 0$ and $|V^B W| \geqslant 2$. Thus $W = V^B$.

Applications to Hilbert's Tenth Problem

The 9 Unknowns Theorem (Matiyasevich, 1975). There is no algorithm to determine for any $P(x_1, \ldots, x_9) \in \mathbb{Z}[x_1, \ldots, x_9]$ whether $P(x_1, \ldots, x_9) = 0$ has solutions with $x_1, \ldots, x_9 \in \mathbb{N}$.

The 11 Unknowns Theorem (Z.-W. Sun [Sci. China Math. 64 (2021)]) There is no algorithm to determine for any $P(z_1, \ldots, z_{11}) \in \mathbb{Z}[z_1, \ldots, z_{11}]$ whether the equation

$$P(z_1, \ldots, z_{11}) = 0$$

has integral solutions.

References

For main sources of my work mentioned here, you may look at:

1. Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Math. 35(1992), 257–269.

2. Z.-W. Sun, *Further results on Hilbert's Tenth Problem*, Sci. China Math. **64** (2021), 281–306.

Thank you!