On The Discriminator of Lucas Sequences

Bernadette Faye
Ph.D Student

FraZA, Bordeaux

November 8, 2017

The Discriminator

Let $\mathbf{a} = \{a_n\}_{n\geq 1}$ be a sequence of distinct integers. The *Discriminator* is defined as

$$\mathcal{D}_{\mathbf{a}}(n) = \min\{m : a_0, \ldots, a_{n-1} \text{ are pairwise distinct modulo } m\}.$$

The Discriminator

Example

- For $\mathbf{a} = \{1, 2, 8, 14\}, \;\; \mathcal{D}_{\mathbf{a}} = 5$.

The Discriminator

Example

- For $\mathbf{a} = \{1, 2, 8, 14\}$, $\mathcal{D}_{\mathbf{a}} = 5$.
- For $\mathbf{a} = \{1^2, 2^2, 3^2, 4^2, 5^2\}$, $\mathcal{D}_{\mathbf{a}} = 10$.

The Discriminator

Problem

Give an easy description or characterization of the Discriminator.

The Discriminator

Problem

Give an easy description or characterization of the Discriminator.

Remark: $\mathcal{D}_{\mathbf{a}}(n) \geq n$.

Motivation: A problem in computer simulation

- Let $S = \{1^2, 2^2, ..., n^2\}$ be a set of integers. Compute the square roots of its elements.

Motivation: A problem in computer simulation

- Let $S = \{1^2, 2^2, ..., n^2\}$ be a set of integers. Compute the square roots of its elements.
- Solution: Take A be a $1 \times n^2$ array with $A(x) = x^{1/2}$. For any value $s \in S, A(s)$ is the square root of s.

Motivation: A problem in computer simulation

- Let $S = \{1^2, 2^2, ..., n^2\}$ be a set of integers. Compute the square roots of its elements.
- Solution: Take A be a $1 \times n^2$ array with $A(x) = x^{1/2}$. For any value $s \in S, A(s)$ is the square root of s.
- **modulo function:** if $1^2, 2^2, ..., n^2$ are distinct modulo k, then letting $A(r) = x^{1/2}$ with $r \equiv x \mod k$ and $1 \leq r \leq k$ allow the same look up procedure to be performed.

Motivation: A problem in computer simulation

- Let $S = \{1^2, 2^2, ..., n^2\}$ be a set of integers. Compute the square roots of its elements.
- Solution: Take A be a $1 \times n^2$ array with $A(x) = x^{1/2}$. For any value $s \in S, A(s)$ is the square root of s.
- **modulo function:** if $1^2, 2^2, ..., n^2$ are distinct modulo k, then letting $A(r) = x^{1/2}$ with $r \equiv x \mod k$ and $1 \leq r \leq k$ allow the same look up procedure to be performed.

History

Theorem (Arnold, Benkoski, McCabe (1985))

If $n > 4$, *and* $\mathbf{a} = \{1^2, 2^2, \ldots, n^2\}$

$$D_{\mathbf{a}}(n) = \min\{m \geq 2n : m = p \text{ or } m = 2p \quad \text{with } p \text{ an odd prime}\}.$$

History

- Bremser, Schumer and Washington (1990): for a cycle polynomial $f = x^d$ and d is odd,

$$D_f(n) = \min\{k \geq n : f : \mathbb{Z}/k\mathbb{Z} \mapsto \mathbb{Z}/k\mathbb{Z} \quad \text{is a permutation}\}$$

History

- Bremser, Schumer and Washington (1990): for a cycle polynomial $f = x^d$ and d is odd,

$$D_f(n) = \min\{k \geq n : f : \mathbb{Z}/k\mathbb{Z} \mapsto \mathbb{Z}/k\mathbb{Z} \quad \text{is a permutation}\}$$

- Moree and Mullen (1996): when f is a Dickson polynomial of degree coprime to 6.

On function taking only prime values

Theorem (Zhi-Wei Sun, 2013)

For $n \in \mathbb{Z}^+$ *let* $S(n)$ *denote the smallest integer* $m > 1$ *such that those* $2k(k-1)$ *modulo* m *for* $k = 1, \ldots, n$ *are pairwise distinct. Then* $S(n)$ *is the least prime greater than* $2n - 2$.

On function taking only prime values

Theorem (Zhi-Wei Sun, 2013)

For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ modulo m for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n-2$.

Fact

$S(n)$ is exactly the set of all prime numbers!

On function taking only prime values

Theorem (Zhi-Wei Sun, 2013)

For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ modulo m for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n-2$.

Fact

$S(n)$ is exactly the set of all prime numbers!

Remark

The way to generate all primes via this theorem is simple in concept, but it has no advantage in algorithm. Nevertheless, it is of certain theoretical interest since it provides a surprising new characterization of primes.

Discriminator for non polynomial sequences

- Moree and Zumalacárregui(2016) :
  $u(j) = \frac{3^j - 5(-1)^j}{4}, \ j = 1, 2, 3, \ldots$

$$D_u(n) := \min\{2^e, 5^f\},$$

where $e = \lceil \log_2(n) \rceil$ and $f = \lceil \log_5(5n/4) \rceil$.

Discriminator for non polynomial sequences

- Moree and Zumalacárregui(2016) :
  $u(j) = \frac{3^j - 5(-1)^j}{4}, \; j = 1, 2, 3, \ldots$

  $$D_u(n) := \min\{2^e, 5^f\},$$

  where $e = \lceil \log_2(n) \rceil$ and $f = \lceil \log_5(5n/4) \rceil$.

- Ciolan and Moree(Preprint arxiv 2017): For every prime $q \geq 7$, the discriminator of the family

  $$u_q(j) = \frac{3^j - q(-1)^{j+(q-1)/2}}{4}, \; j = 1, 2, 3, \ldots$$

Shallit's Conjecture

In May 2016, Jeffrey Shallit posed the following conjecture.

Conjecture: Given $k \geq 1$, consider the recurrence with numbers determined by

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n), \qquad u_k(0) = 0,\ u_k(1) = 1.$$

Shallit's Conjecture

In May 2016, Jeffrey Shallit posed the following conjecture.

Conjecture: Given $k \geq 1$, consider the recurrence with numbers determined by

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n), \qquad u_k(0) = 0, \; u_k(1) = 1.$$

Then, for $k \leq 6$, the discriminator $D_k(n)$ of the sequence $u_k(n)$ is the smallest number $m \geq n$ taken from the sets $\mathcal{D}_k$ defined as.

Shallit's Conjecture

In May 2016, Jeffrey Shallit posed the following conjecture.

Conjecture: Given $k \geq 1$, consider the recurrence with numbers determined by

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n), \qquad u_k(0) = 0,\ u_k(1) = 1.$$

Then, for $k \leq 6$, the discriminator $D_k(n)$ of the sequence $u_k(n)$ is the smallest number $m \geq n$ taken from the sets $\mathcal{D}_k$ defined as.

$$\begin{aligned}
\mathcal{D}_1 &= \{2^i, 250 \cdot 2^i\}. \\
\mathcal{D}_2 &= \{2^i, 3 \cdot 2^i\}. \\
\mathcal{D}_3 &= \{2^i \cdot 3^j\}. \\
\mathcal{D}_4 &= \{2^i \cdot 5^{j+1}\}. \\
\mathcal{D}_5 &= \{2^{i+1} \cdot 3^j \cdot 5^l\}. \\
\mathcal{D}_6 &= \{2^{i+1} \cdot 3^j \cdot 7^l\}.
\end{aligned}$$

Case $k = 1$

Theorem (Moree, Luca, F. (2017))

Let v_n be the smallest power of two such that $v_n \geq n$. Let w_n be the smallest integer of the form 2^a5^b satisfying $2^a5^b \geq 5n/3$ with $a, b \geq 1$. Then

$$\mathcal{D}_1(n) = \min\{v_n, w_n\}.$$

Case $k = 1$

Theorem (Moree, Luca, F. (2017))

Let v_n be the smallest power of two such that $v_n \geq n$. Let w_n be the smallest integer of the form $2^a 5^b$ satisfying $2^a 5^b \geq 5n/3$ with $a, b \geq 1$. Then

$$\mathcal{D}_1(n) = \min\{v_n, w_n\}.$$

Let

$$\mathcal{M} = \left\{ m \geq 1 : \left\{ m \frac{\log 5}{\log 2} \right\} \geq 1 - \frac{\log(6/5)}{\log 2} \right\} = \{3, 6, 9, 12, 15, \ldots\}.$$

Case $k = 1$

Theorem (Moree, Luca, F. (2017))

Let v_n be the smallest power of two such that $v_n \geq n$. Let w_n be the smallest integer of the form $2^a 5^b$ satisfying $2^a 5^b \geq 5n/3$ with $a, b \geq 1$. Then

$$\mathcal{D}_1(n) = \min\{v_n, w_n\}.$$

Let

$$\mathcal{M} = \left\{ m \geq 1 : \left\{ m \frac{\log 5}{\log 2} \right\} \geq 1 - \frac{\log(6/5)}{\log 2} \right\} = \{3, 6, 9, 12, 15, \ldots\}.$$

We have

$$\{\mathcal{D}_1(2), \mathcal{D}_1(3), \mathcal{D}_1(4), \ldots\} = \{2^a 5^b : a \geq 1,\ b \in \mathcal{M} \cup \{0\}\}.$$

Case $k = 2$

Theorem (Moree, Luca, F. (2017))

Let $e \geq 0$ *be the smallest integer such that* $2^e \geq n$ *and* $f \geq 1$ *the smallest integer such that* $3 \cdot 2^f \geq n$*. Then* $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$*.*

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \equiv 6 \pmod 9, \end{cases}$$

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \ \text{then } p \mid k\} \text{ if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \ \text{then } p \mid k\} \text{ if } k \equiv 6 \pmod 9, \end{cases}$$

and

$$\mathcal{B}_k = \begin{cases} \{m \text{ even} : \text{if } p \mid m, \ \text{then } p \mid k(k+1)\} \text{ if } k \not\equiv 2 \pmod 9; \\ \{m \text{ even}, \ 9 \nmid m : \text{if } p \mid m, \ \text{then } p \mid k(k+1)\} \text{ if } k \equiv 2 \pmod 9. \end{cases}$$

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \equiv 6 \pmod 9, \end{cases}$$

and

$$\mathcal{B}_k = \begin{cases} \{m \text{ even} : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \not\equiv 2 \pmod 9; \\ \{m \text{ even}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \equiv 2 \pmod 9. \end{cases}$$

Let $k > 2$. We have

$$\mathcal{D}_k(n) \leq \min\{m \geq n : m \in \mathcal{A}_k \cup \mathcal{B}_k\},$$

with equality if the interval $[n, 3n/2)$ contains an integer $m \in \mathcal{A}_k \cup \mathcal{B}_k$ and with at most finitely many n for which strict inequality holds.

Main Tools

The main tools used for the proof of Shallit's conjecture are:

- properties of a binary recurrent sequence $\{u_n\}_{n\geq 0}$,

Main Tools

The main tools used for the proof of Shallit's conjecture are:

- properties of a binary recurrent sequence $\{u_n\}_{n\geq 0}$,
- order of appearance $z(m)$ of an integer m is the sequence u_n,

$$U_0, U_1, \ldots, U_{z(m)}, \ldots,$$

Main Tools

The main tools used for the proof of Shallit's conjecture are:

- properties of a binary recurrent sequence $\{u_n\}_{n\geq 0}$,
- order of appearance $z(m)$ of an integer m is the sequence u_n,

$$U_0, U_1, \ldots, U_{z(m)}, \ldots,$$

$$U_i \not\equiv 0 \pmod{m}, i \in [0, z(m)-1] \quad \text{but} \quad U_{z(m)} \equiv 0 \pmod{m}.$$

Method of the Proof

- Find an interval for the $D_{\mathbf{u}}(n)$: for example if 2^e is a discriminator, then

$$2^e \geq n, \quad \text{and,} \quad D_{\mathbf{u}}(n) \in [n, 2n].$$

Method of the Proof

- Find an interval for the $D_{\mathbf{u}}(n)$: for example if 2^e is a discriminator, then

$$2^e \geq n, \quad \text{and}, \quad D_{\mathbf{u}}(n) \in [n, 2n].$$

- Find a form for an eligible or ineligible value of the discriminator: For example, we consider

$$a_0, a_1, \ldots, a_{n-1},$$

with $a_0 = 0$. For an integer k to be a discriminant, $z(k) \geq n$.

Method of the Proof

- Find a form for an eligible or ineligible value of the discriminator: For example, we consider

$$a_0, a_1, \dots, a_{n-1},$$

with $a_0 = 0$. For an integer k to be a discriminant, $z(k) \geq n$.

Method of the Proof

- Find a form for an eligible or ineligible value of the discriminator: For example, we consider

$$a_0, a_1, \ldots, a_{n-1},$$

  with $a_0 = 0$. For an integer k to be a discriminant, $z(k) \geq n$.

- Study the congruence relation $U_i \equiv U_j \pmod{k}$.

Sketch of the Proofs
The congruence $U_i \equiv U_j \pmod{k}$

Consider the sequence

$$U_0, U_1, \ldots, U_{n-1}.$$

Sketch of the Proofs
The congruence $U_i \equiv U_j \pmod{k}$

Consider the sequence

$$U_0, U_1, \ldots, U_{n-1}.$$

If k is a discriminator, then

$$U_i \not\equiv U_j \pmod{k} \quad \text{for} \quad 0 \le i, j \le n-1$$

Sketch of the Proofs
The congruence $U_i \equiv U_j \pmod{k}$

Consider the sequence

$$U_0, U_1, \ldots, U_{n-1}.$$

If k is a discriminator, then

$$U_i \not\equiv U_j \pmod{k} \quad \text{for} \quad 0 \le i, j \le n-1$$

Otherwise, $\exists (i,j) \in [0, n-1]$ such that

$$U_i \equiv U_j \pmod{k}.$$

$$\implies k \mid U_i - U_j.$$

Some properties of Lucas recurrent sequences

We consider the Lucas sequence $\{u_n\}_{n\geq 0}$, with $u_0 = 0,\ u_1 = 1$ and

$$u_{n+2} = ru_{n+1} + su_n \qquad \text{for all} \qquad n \geq 0, \tag{1}$$

where $s = -1$ and $r := 4k + 2$ are integers. Put $\Delta = r^2 - 4$ and assume that $\Delta \neq 0$.

Some properties of Lucas recurrent sequences

We consider the Lucas sequence $\{u_n\}_{n\geq 0}$, with $u_0 = 0, \; u_1 = 1$ and

$$u_{n+2} = ru_{n+1} + su_n \qquad \text{for all} \qquad n \geq 0, \tag{1}$$

where $s = -1$ and $r := 4k + 2$ are integers. Put $\Delta = r^2 - 4$ and assume that $\Delta \neq 0$.
Let (α, β) be the roots of the characteristic equation $x^2 - rx + 1 = 0$ of the binary sequence $\{u_n\}_{n\geq 0}$, then the so-called Binet formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{holds for all} \quad n \geq 0. \tag{2}$$

We let $\{v_n\}_{n\geq 0}$ for the companion Lucas sequence of $\{u_n\}_{n\geq 0}$ given by $v_0 = 2,\ v_1 = r$ and $v_{n+2} = rv_{n+1} - v_n$. Its Binet formula is

$$v_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \geq 0. \tag{3}$$

We let $\{v_n\}_{n\geq 0}$ for the companion Lucas sequence of $\{u_n\}_{n\geq 0}$ given by $v_0 = 2,\ v_1 = r$ and $v_{n+2} = rv_{n+1} - v_n$. Its Binet formula is

$$v_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \geq 0. \tag{3}$$

Lemma

Let i and j be two integers with the same parity i.e $i \equiv j \pmod 2$. Then

$$u_i - u_j = u_{(i-j)/2} v_{(i+j)/2}.$$

We let $\{v_n\}_{n\geq 0}$ for the companion Lucas sequence of $\{u_n\}_{n\geq 0}$ given by $v_0 = 2,\ v_1 = r$ and $v_{n+2} = rv_{n+1} - v_n$. Its Binet formula is

$$v_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \geq 0. \tag{3}$$

Lemma

Let i and j be two integers with the same parity i.e $i \equiv j \pmod 2$. Then

$$u_i - u_j = u_{(i-j)/2} v_{(i+j)/2}.$$

Lemma (Bertrand's Postulate(1845))

For every natural number $n > 3$, there is a prime p satisfying $n < p < 2n$.

Index of appearance $z(m)$

Lemma (Bilu, Hanrot, Voutier (2001).)

The index of appearance z of the sequence $U(k)$ has the following properties.

i) *If $p \mid \Delta(k)$, then $z(p) = p$.*

ii) *If $p \nmid \Delta(k)$, then $z(p) \mid p - e$, where $e = (\frac{\Delta(k)}{p})$.*

iii) *Let $c = \nu_p(U_{z(p)}(k))$. Then $z(p^b) = p^{\max\{b-c,0\}} z(p)$.*

iv) *If $p | U_m(k)$, then $z(p) | m$.*

v) *If $n = m_1 \cdots m_s$ with $m_1, \ldots, m_s$ pairwise coprime, then*

$$z(m_1 \cdots m_s) = \mathrm{lcm}[z(m_1), \ldots, z(m_s)].$$

Steps of the Proof for $k = 1$

In this case, we consider the binary recurrent sequence $\{u_n\}_{n\geq 0}$ given by $u_0 = 0$, $u_1 = 1$ and $u_{n+1} = 6u_n - u_{n-1}$ for all $n \geq 0$. Its first terms are

$$0, 1, 6, 35, 204, 1189, 6930, 40391, 235416, 1372105, 7997214, \ldots.$$

Steps of the Proof for $k = 1$

In this case, we consider the binary recurrent sequence $\{u_n\}_{n\geq 0}$ given by $u_0 = 0$, $u_1 = 1$ and $u_{n+1} = 6u_n - u_{n-1}$ for all $n \geq 0$. Its first terms are

$$0, 1, 6, 35, 204, 1189, 6930, 40391, 235416, 1372105, 7997214, \ldots.$$

Result: $D_u(n) = \min\{2^e, 2^a \cdot 5^b\}$, with $2^a 5^b \geq 5n/3$.

Step 1: Structure of $D_1(n)$

Lemma

Let $m = \mathcal{D}_1(n)$ for some $n > 1$. Then

i) *m has at most one odd prime divisor.*

ii) *If m is divisible by exactly one odd prime p, then $e = \left(\frac{2}{p}\right) = -1$ and $z(p) = (p+1)/2$.*

iii) *If m is not a power of 2, then m can be written as $2^a p^b$ with $a, b \geq 1$ and $p \equiv 5 \pmod 8$.*

Step 1: Structure of $D_1(n)$

Lemma

Let $m = \mathcal{D}_1(n)$ for some $n > 1$. Then

i) *m has at most one odd prime divisor.*

ii) *If m is divisible by exactly one odd prime p, then $e = \left(\frac{2}{p}\right) = -1$ and $z(p) = (p+1)/2$.*

iii) *If m is not a power of 2, then m can be written as $2^a p^b$ with $a, b \geq 1$ and $p \equiv 5 \pmod 8$.*

Lemma

Assume that $m = 2^a p_1^{b_1}$ is such that $a \geq 1$, $p_1 \equiv 5 \pmod 8$ and $z(p_1) = (p_1 + 1)/2$. Then $U_i \equiv U_j \pmod m$ holds if and only if $i \equiv j \pmod{z(m)}$.

Proof

- Assume that $\mathcal{D}_1(n) = m$ and write it as

$$m = 2^a p_1^{b_1} \cdots p_r^{b_r},$$

where the p_i are distinct odd primes.

Proof

- Assume that $\mathcal{D}_1(n) = m$ and write it as

$$m = 2^a p_1^{b_1} \cdots p_r^{b_r},$$

  where the p_i are distinct odd primes.
- If $r \geq 2$, we obtain the inequality

$$z(m) \leq 2^a p_1^{b_1 - 1} \cdots p_r^{b_k - 1} \left(\frac{p_1 + 1}{2}\right) \cdots \left(\frac{p_r + 1}{2}\right) < \frac{m}{2}, \quad (4)$$

Proof

- Assume that $\mathcal{D}_1(n) = m$ and write it as

$$m = 2^a p_1^{b_1} \cdots p_r^{b_r},$$

  where the p_i are distinct odd primes.
- If $r \geq 2$, we obtain the inequality

$$z(m) \leq 2^a p_1^{b_1 - 1} \cdots p_r^{b_k - 1} \left(\frac{p_1 + 1}{2} \right) \cdots \left(\frac{p_r + 1}{2} \right) < \frac{m}{2}, \quad (4)$$

- it follows that the interval $[z(m), 2z(m))$ contains a power of 2, say $2^b < 2z(m) < m$. But then since $2^b \geq z(m) \geq n$, we get a contradiction.

Proof

- Assume that $\mathcal{D}_1(n) = m$ and write it as

$$m = 2^a p_1^{b_1} \cdots p_r^{b_r},$$

where the p_i are distinct odd primes.

- If $r \geq 2$, we obtain the inequality

$$z(m) \leq 2^a p_1^{b_1 - 1} \cdots p_r^{b_k - 1} \left(\frac{p_1 + 1}{2} \right) \cdots \left(\frac{p_r + 1}{2} \right) < \frac{m}{2}, \quad (4)$$

- it follows that the interval $[z(m), 2z(m))$ contains a power of 2, say $2^b < 2z(m) < m$. But then since $2^b \geq z(m) \geq n$, we get a contradiction.
- If $r = 1$ and $e_1 = (\frac{2}{p_1}) = 1$, then

$$z(m) = z(2^a p_1^{b_1}) \leq 2^a p_1^{b_1 - 1}(p_1 - 1)/2 < m/2,$$

a contradiction

- Assume now that $e_1 = -1$ and that $z(p_1)$ is a proper divisor of $(p+1)/2$. Then

$$z(m) \le 2^a p_1^{b_1-1} z(p_1) \le 2^a p_1^{b_1-1}(p_1+1)/4 < m/2,$$

again the same contradiction.

- Assume now that $e_1 = -1$ and that $z(p_1)$ is a proper divisor of $(p+1)/2$. Then

$$z(m) \le 2^a p_1^{b_1 - 1} z(p_1) \le 2^a p_1^{b_1 - 1}(p_1 + 1)/4 < m/2,$$

again the same contradiction.
- We write $m = 2^a p_1^{b_1}$. We know that $a \ge 1$ and $e = -1$. Thus, $p \equiv \pm 3 \pmod 8$. If $p \equiv 3 \pmod 8$, then

$$z(m) = \mathrm{lcm}[z(2^a), z(p^b)] \mid 2^a p^{b-1}(p+1)/4.$$

In particular, $z(m) < m/2$, and we get again a contradiction. Thus, $p \equiv 5 \pmod 8$.

Step 2

Lemma

For $n \geq 2^{24} \cdot 5^3$ *the interval* $[5n/3, 37n/19)$ *contains a number of the form* $2^a \cdot 5^b$ *with* $a \geq 1$ *and* $b \geq 0$.

Step 2

Lemma

For $n \geq 2^{24} \cdot 5^3$ the interval $[5n/3, 37n/19)$ contains a number of the form $2^a \cdot 5^b$ with $a \geq 1$ and $b \geq 0$.

Corollary

Suppose that $m = 2^a \cdot p^b$, $p > 5$, $a, b \geq 1$. If $m \geq \frac{37}{19} \cdot 2^{24} \cdot 5^3$, then m is not a discriminator value.

Step 2

Lemma
For $n \geq 2^{24} \cdot 5^3$ the interval $[5n/3, 37n/19)$ contains a number of the form $2^a \cdot 5^b$ with $a \geq 1$ and $b \geq 0$.

Corollary
Suppose that $m = 2^a \cdot p^b$, $p > 5$, $a, b \geq 1$. If $m \geq \frac{37}{19} \cdot 2^{24} \cdot 5^3$, then m is not a discriminator value.

- Suppose that $\mathcal{D}_1(n) = m$, then we must have

$$z(m) = 2^a \cdot p^{b-1}(p+1)/(2) \geq 19m/37 \geq n,$$

that is $m \geq 37n/19$; a contradiction

Step 3

Lemma

We say that m discriminates $U_0, \ldots, U_{n-1}$ if these integers are pairwise distinct modulo m.

i) *The integer $m = 2^a$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq n$.*

Step 3

Lemma

We say that m discriminates $U_0, \ldots, U_{n-1}$ if these integers are pairwise distinct modulo m.

i) *The integer $m = 2^a$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq n$.*

ii) *The integer $m = 2^a \cdot 5^b$ with $a, b \geq 1$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq 5n/3$.*

Step 3

Lemma

We say that m discriminates $U_0, \ldots, U_{n-1}$ if these integers are pairwise distinct modulo m.

i) *The integer $m = 2^a$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq n$.*

ii) *The integer $m = 2^a \cdot 5^b$ with $a, b \geq 1$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq 5n/3$.*

Proof.

- m discriminates $U_0, \ldots, U_{z(m)-1}$, but not $U_0, \ldots, U_{z(m)}$.

Step 3

Lemma

We say that m discriminates $U_0, \ldots, U_{n-1}$ if these integers are pairwise distinct modulo m.

i) *The integer $m = 2^a$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq n$.*

ii) *The integer $m = 2^a \cdot 5^b$ with $a, b \geq 1$ discriminates $U_0, \ldots, U_{n-1}$ if and only if $m \geq 5n/3$.*

Proof.

- m discriminates $U_0, \ldots, U_{z(m)-1}$, but not $U_0, \ldots, U_{z(m)}$.
- then m discriminates $U_0, \ldots, U_{n-1}$ iff $n \leq z(m)$.

Step 3

Lemma

We say that m discriminates $U_0, \dots, U_{n-1}$ if these integers are pairwise distinct modulo m.

i) *The integer $m = 2^a$ discriminates $U_0, \dots, U_{n-1}$ if and only if $m \geq n$.*

ii) *The integer $m = 2^a \cdot 5^b$ with $a, b \geq 1$ discriminates $U_0, \dots, U_{n-1}$ if and only if $m \geq 5n/3$.*

Proof.

- m discriminates $U_0, \dots, U_{z(m)-1}$, but not $U_0, \dots, U_{z(m)}$.
- then m discriminates $U_0, \dots, U_{n-1}$ iff $n \leq z(m)$.
- As it is easily seen that $z(m) = 3m/5$, the result follows.

□

Case $k = 2$, $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$

.

- if $z(m) = m$, then $m | 3 \cdot 2^a$ for some $a \geq 0$.

Case $k = 2$, $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$

.

- if $z(m) = m$, then $m | 3 \cdot 2^a$ for some $a \geq 0$.
- or $z(m) \leq 3m/5$.

Case $k = 2$, $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$

.

- if $z(m) = m$, then $m | 3 \cdot 2^a$ for some $a \geq 0$.
- or $z(m) \leq 3m/5$.
- if m is a discriminator then $m \geq 5n/3$.

Case $k = 2$, $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$

.

- if $z(m) = m$, then $m | 3 \cdot 2^a$ for some $a \geq 0$.
- or $z(m) \leq 3m/5$.
- if m is a discriminator then $m \geq 5n/3$.
- for $n \geq 2$, there is a power of two or a number of the form $3 \cdot 2^a$ in the interval $[n, 5n/3)$.

Case $k = 2$

Theorem (Moree, Luca, F. (2017))

Let $e \geq 0$ be the smallest integer such that $2^e \geq n$ and $f \geq 1$ the smallest integer such that $3 \cdot 2^f \geq n$. Then $\mathcal{D}_2(n) = \min\{2^e, 3 \cdot 2^f\}$.

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \text{if } k \equiv 6 \pmod 9, \end{cases}$$

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \equiv 6 \pmod 9, \end{cases}$$

and

$$\mathcal{B}_k = \begin{cases} \{m \text{ even} : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \not\equiv 2 \pmod 9; \\ \{m \text{ even}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \equiv 2 \pmod 9. \end{cases}$$

Case $k > 2$

Theorem (Moree, Luca, F. (2017))

Put

$$\mathcal{A}_k = \begin{cases} \{m \text{ odd} : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \not\equiv 6 \pmod 9; \\ \{m \text{ odd}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k\} & \textit{if } k \equiv 6 \pmod 9, \end{cases}$$

and

$$\mathcal{B}_k = \begin{cases} \{m \text{ even} : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \not\equiv 2 \pmod 9; \\ \{m \text{ even}, \ 9 \nmid m : \text{if } p \mid m, \text{ then } p \mid k(k+1)\} & \textit{if } k \equiv 2 \pmod 9. \end{cases}$$

Let $k > 2$. We have

$$\mathcal{D}_k(n) \le \min\{m \ge n : m \in \mathcal{A}_k \cup \mathcal{B}_k\},$$

with equality if the interval $[n, 3n/2)$ contains an integer $m \in \mathcal{A}_k \cup \mathcal{B}_k$ and with at most finitely many n for which strict inequality holds.

Case $k > 2$

Here, we have to consider two cases:

- $p \mid k(k+1)$

Case $k > 2$

Here, we have to consider two cases:

- $p \mid k(k+1)$
- $p \nmid k(k+1)$

The congruence $U_i(k) \equiv U_j(k) \pmod{m}$

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n).$$

- $\Delta(k) = 16k(k+1)$.

The congruence $U_i(k) \equiv U_j(k) \pmod{m}$

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n).$$

- $\Delta(k) = 16k(k+1)$.
- $k(k+1) = du^2$, and let $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$.

The congruence $U_i(k) \equiv U_j(k) \pmod{m}$

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n).$$

- $\Delta(k) = 16k(k+1)$.
- $k(k+1) = du^2$, and let $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$.
- Let $p^a || k$ and π be any prime ideal diving p and let e be such that $\pi^e \| p$.

The congruence $U_i(k) \equiv U_j(k) \pmod{m}$

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n).$$

- $\Delta(k) = 16k(k+1)$.
- $k(k+1) = du^2$, and let $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$.
- Let $p^a \| k$ and π be any prime ideal diving p and let e be such that $\pi^e \| p$.
- We assume $U_i \equiv \lambda \pmod{p^b}$ then

$$\alpha^i - \alpha^{-i} - 4\sqrt{k(k+1)}\lambda \equiv 0 \pmod{\pi^{eb+ae/2}}.$$

The congruence $U_i(k) \equiv U_j(k) \pmod{m}$

$$u_k(n+2) = (4k+2)u_k(n+1) - u_k(n).$$

- $\Delta(k) = 16k(k+1)$.
- $k(k+1) = du^2$, and let $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$.
- Let $p^a || k$ and π be any prime ideal diving p and let e be such that $\pi^e \| p$.
- We assume $U_i \equiv \lambda \pmod{p^b}$ then

$$\alpha^i - \alpha^{-i} - 4\sqrt{k(k+1)}\lambda \equiv 0 \pmod{\pi^{eb+ae/2}}.$$

- then it satisfied the quadratic congruence

$$x^2 - 4\sqrt{k(k+1)}\lambda x - 1 = 0 \pmod{\pi^{eb+ae/2}}.$$

- Taking their difference we get

$$(\alpha^i - \alpha^j)(\alpha^i + \alpha^j - 4\sqrt{k(k+1)})\lambda \equiv 0 \pmod{\pi^{be+ae/2}}.$$

- Taking their difference we get

$$(\alpha^i - \alpha^j)(\alpha^i + \alpha^j - 4\sqrt{k(k+1)})\lambda \equiv 0 \pmod{\pi^{be+ae/2}}.$$

- If $p \mid k$, we have that

$$\alpha = 2k + 1 + 2\sqrt{k(k+1)} \equiv 1 \pmod{\pi}.$$

Then

$$(\alpha^i + \alpha^j - 4\sqrt{k(k+1)}) \equiv 2 \pmod{\pi^{ae/2}}$$

- Taking their difference we get

$$(\alpha^i - \alpha^j)(\alpha^i + \alpha^j - 4\sqrt{k(k+1)})\lambda \equiv 0 \pmod{\pi^{be+ae/2}}.$$

- If $p \mid k$, we have that

$$\alpha = 2k + 1 + 2\sqrt{k(k+1)} \equiv 1 \pmod{\pi}.$$

Then

$$(\alpha^i + \alpha^j - 4\sqrt{k(k+1)}) \equiv 2 \pmod{\pi^{ae/2}}$$

- Thus,

$$\alpha^i \equiv \alpha^j \pmod{\pi^{be+ae/2}}$$

- Taking their difference we get

$$(\alpha^i - \alpha^j)(\alpha^i + \alpha^j - 4\sqrt{k(k+1)})\lambda \equiv 0 \pmod{\pi^{be+ae/2}}.$$

- If $p \mid k$, we have that

$$\alpha = 2k + 1 + 2\sqrt{k(k+1)} \equiv 1 \pmod{\pi}.$$

  Then

$$(\alpha^i + \alpha^j - 4\sqrt{k(k+1)}) \equiv 2 \pmod{\pi^{ae/2}}$$

- Thus,

$$\alpha^i \equiv \alpha^j \pmod{\pi^{be+ae/2}}$$

- This give $\pi^{eb} \mid U_{i-j}$ and

$$i - j \equiv 0 \pmod{z(p^b)}$$

.

Lemma

Assume $p \mid k$ *is odd. Then* $U_i \equiv U_j \pmod{p^b}$ *if and only if* $i \equiv j \pmod{z(p^b)}$.

- If $p \mid (k+1)$, we have that the factors

$$(\alpha^i - \alpha^j) \quad \text{and} \quad (\alpha^i + \alpha^j - 4\sqrt{k(k+1)})$$

$\equiv (-1)^i + (-1)^j \pmod{\pi^{ae/2}}$.

- If $p \mid (k+1)$, we have that the factors

$$(\alpha^i - \alpha^j) \quad \text{and} \quad (\alpha^i + \alpha^j - 4\sqrt{k(k+1)})$$

$\equiv (-1)^i + (-1)^j \pmod{\pi^{ae/2}}$.

- Thus, π never divides both factors, and $\pi^{ae/2}$ divides $\alpha^i - \alpha^j$ in case $i \equiv j \pmod 2$, and it divides $\alpha^i + \alpha^j - 4\sqrt{k(k+1)}\lambda$ in case $i \not\equiv j \pmod 2$.

Lemma

Assume that p *is odd and* $p \mid (k+1)$*. Then* $U_i \equiv U_j \pmod{p^b}$ *is equivalent to one of the following:*

i) *If* $i \equiv j \pmod{2}$*, then* $i \equiv j \pmod{z(p^b)}$*.*

Lemma

Assume that p is odd and $p \mid (k+1)$. *Then* $U_i \equiv U_j \pmod{p^b}$ *is equivalent to one of the following:*

i) *If* $i \equiv j \pmod{2}$, *then* $i \equiv j \pmod{z(p^b)}$.

ii) *If* $i \not\equiv j \pmod{2}$, *then* $i + j \equiv 0 \pmod{z(p^b)}$.

Lemma

We have

$$i \equiv j \pmod{m} \iff U_i \equiv U_j \pmod{m}, \tag{5}$$

precisely when

$$m \in \mathcal{A}_k \cup \mathcal{B}_k.$$

Lemma

We have

$$i \equiv j \pmod{m} \iff U_i \equiv U_j \pmod{m}, \qquad (5)$$

precisely when

$$m \in \mathcal{A}_k \cup \mathcal{B}_k.$$

- $\{m \text{ odd} : z(m) = m \text{ and } m \in \mathcal{P}(k)\}$.
- $\{m \text{ even} : z(m) = m\}$.

The set $\mathcal{F}_k$

For $k > 1$ there is a finite set $\mathcal{F}_k$ such that

$$\mathcal{D}_k = \mathcal{A}_k \cup \mathcal{B}_k \cup \mathcal{F}_k.$$

Lemma

There are infinitely many k for the finite set $\mathcal{F}_k$ is non-empty. It can have a cardinality larger than any given bound.

The set $\mathcal{F}_k$

For $k > 1$ there is a finite set $\mathcal{F}_k$ such that

$$\mathcal{D}_k = \mathcal{A}_k \cup \mathcal{B}_k \cup \mathcal{F}_k.$$

- $\mathcal{A}_1 = \{1\},\ \mathcal{B}_1 = \{2^e : e \geq 1\}$

$$\mathcal{F}_1 = \{2^a \cdot 5^m : a \geq 1 \text{ and } m \in \mathcal{M}\}.$$

The set $\mathcal{F}_k$

For $k > 1$ there is a finite set $\mathcal{F}_k$ such that

$$\mathcal{D}_k = \mathcal{A}_k \cup \mathcal{B}_k \cup \mathcal{F}_k.$$

- $\mathcal{A}_1 = \{1\},\ \mathcal{B}_1 = \{2^e : e \geq 1\}$

$$\mathcal{F}_1 = \{2^a \cdot 5^m : a \geq 1 \text{ and } m \in \mathcal{M}\}.$$

- $\mathcal{F}_2$ is empty.

The set $\mathcal{F}_k$

For $k > 1$ there is a finite set $\mathcal{F}_k$ such that

$$\mathcal{D}_k = \mathcal{A}_k \cup \mathcal{B}_k \cup \mathcal{F}_k.$$

- $\mathcal{A}_1 = \{1\},\ \mathcal{B}_1 = \{2^e : e \geq 1\}$

$$\mathcal{F}_1 = \{2^a \cdot 5^m : a \geq 1 \text{ and } m \in \mathcal{M}\}.$$

- $\mathcal{F}_2$ is empty.
- $\mathcal{F}_k$ is finite for $k > 1$.

Example

For $k = 3$, we have the following sequence $u_{n+1} = 14u_n - u_{n-1}$ for all $n \geq 0$. Its first terms are

$$0, 1, 14, 195, 2716, 37829, 526890, 7338631 \ldots.$$

The discriminator for $n = 1 \ldots, 20$.

$$D(1) = 1 \qquad D(11) = 2^2 \cdot 3$$
$$D(2) = 2 \qquad D(12) = 2^2 \cdot 3$$
$$D(3) = 3 \qquad D(13) = 2^4$$
$$D(4) = 2^2 \qquad D(14) = 2^4$$
$$D(5) = 2 \cdot 3 \qquad D(15) = 2^4$$
$$D(6) = 2 \cdot 3 \qquad D(16) = 2^4$$
$$D(7) = 2^3 \qquad D(17) = 2 \cdot 3^2$$
$$D(8) = 2^3 \qquad D(18) = 2 \cdot 3^2$$
$$D(9) = 3^2 \qquad D(19) = 2^3 \cdot 3$$
$$D(10) = 2^2 \cdot 3 \qquad D(20) = 2^3 \cdot 3$$

Open Problems

- Give a characterization of $D_u(n)$ for a given Lucas sequence u_n: Fibonacci sequence, Prime numbers sequence, etc.

$$D_P(n) \leq \frac{P_n + 1}{2}.$$

- Give a classification of all recurrent sequence with $D_{|u|}(2^e) = 2^e$

$$D_{|u|}(2^e) = 2^e \implies D_{|u|} \in [n, 2n]$$

Open Problems

Conjecture:

Let $\{u_n\}_{n\geq 0}$ be a binary sequence given by the recurrence

$$\begin{cases} u_0 = a \\ u_1 = b \\ u_{n+2} = r u_{n+1} + s u_n \text{ for } n \geq 0 \end{cases}$$

where r, s are two integers such that $r > 0$ and $(r, s) \neq (2, -1), (1, -1)$. For all $e \geq 1$,

$$D_u(2^e) = 2^e \iff \nu_2(r) = 1, s \equiv 3 \pmod 4$$

and a, b have different parity.

"I love mathematics for its own sake, because it allows for no hypocrisy and no vagueness." Stendhal

THANKS FOR YOUR ATTENTION !