A curious collection of creative conundrums

Mike Daas

Universiteit Leiden

13 mei 2024

Universiteit Leiden

Plan for today

Plan for today

Let's be honest.

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Today, I will discuss three problems that I came up with:

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Today, I will discuss three problems that I came up with:

- Monic polynomials that vanish $\mod m$;

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Today, I will discuss three problems that I came up with:

- Monic polynomials that vanish $\mod m$;
- Scalar endomorphisms in abelian groups;

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Today, I will discuss three problems that I came up with:

- Monic polynomials that vanish $\mod m$;
- Scalar endomorphisms in abelian groups;
- A Collatz-type problem.

Plan for today

Let's be honest.
You are not motivated to work on your PhD project 24/7.
That's okay. Neither am I.
But not working on your maths makes you feel guilty :(
Solution: still work on maths. But fun maths :)

Today, I will discuss three problems that I came up with:

- Monic polynomials that vanish $\mod m$;
- Scalar endomorphisms in abelian groups;
- A Collatz-type problem.

Then I will solve them for you. Just for fun :)

Part 1: Problems

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Answer: $d = 0$, for choose $p(X) = m$ constant. That's boring...

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Answer: $d = 0$, for choose $p(X) = m$ constant. That's boring...

Definition

We say some $p = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[X]$ is *monic* if $a_d = 1$.

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Answer: $d = 0$, for choose $p(X) = m$ constant. That's boring...

Definition

We say some $p = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[X]$ is *monic* if $a_d = 1$.

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a *monic* $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Answer: $d = 0$, for choose $p(X) = m$ constant. That's boring...

Definition

We say some $p = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[X]$ is *monic* if $a_d = 1$.

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a *monic* $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

- Clearly, if $m = 1$, then $p = 1$ works, so $d = 0$.
- If $m = 2$, then

Problem I (1/4)

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a polynomial $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

Answer: $d = 0$, for choose $p(X) = m$ constant. That's boring...

Definition

We say some $p = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[X]$ is *monic* if $a_d = 1$.

Question

Fix $m \in \mathbb{N}$. What is the smallest degree d of a *monic* $p \in \mathbb{Z}[X]$ with with the property that $p(n)$ is divisible by m for all $n \in \mathbb{Z}$?

- Clearly, if $m = 1$, then $p = 1$ works, so $d = 0$.
- If $m = 2$, then $p = X^2 - X$ works, so $d = 2$.
- If $m = 3$, then...?

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

- $X = 0$ gives $b \equiv 0 \mod 3$, so let's say $b = 0$.

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

- $X = 0$ gives $b \equiv 0 \mod 3$, so let's say $b = 0$.
- $X = 1$ gives $1 + a \equiv 0 \mod 3 \implies a \equiv -1 \mod 3$.
- $X = 2$ gives $4 + 2a \equiv 0 \mod 3 \implies a \equiv -2 \mod 3$.

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

- $X = 0$ gives $b \equiv 0 \mod 3$, so let's say $b = 0$.
- $X = 1$ gives $1 + a \equiv 0 \mod 3 \implies a \equiv -1 \mod 3$.
- $X = 2$ gives $4 + 2a \equiv 0 \mod 3 \implies a \equiv -2 \mod 3$.

This is a contradiction, so the answer is *no*.

What about degree 3?

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

- $X = 0$ gives $b \equiv 0 \mod 3$, so let's say $b = 0$.
- $X = 1$ gives $1 + a \equiv 0 \mod 3 \implies a \equiv -1 \mod 3$.
- $X = 2$ gives $4 + 2a \equiv 0 \mod 3 \implies a \equiv -2 \mod 3$.

This is a contradiction, so the answer is *no*.
What about degree 3?
Consider $p = X^3 - X$. Then

$$p(0) = 0, \quad p(1) = 0, \quad \text{and} \quad p(2) = 6.$$

Since $p(X + 3) \equiv p(X) \mod 3$, this is indeed always divisible by 3.

Problem I (2/4)

Can $X^2 + aX + b$ always be divisible by 3?

- $X = 0$ gives $b \equiv 0 \mod 3$, so let's say $b = 0$.
- $X = 1$ gives $1 + a \equiv 0 \mod 3 \implies a \equiv -1 \mod 3$.
- $X = 2$ gives $4 + 2a \equiv 0 \mod 3 \implies a \equiv -2 \mod 3$.

This is a contradiction, so the answer is *no*.
What about degree 3?
Consider $p = X^3 - X$. Then

$$p(0) = 0, \quad p(1) = 0, \quad \text{and} \quad p(2) = 6.$$

Since $p(X+3) \equiv p(X) \mod 3$, this is indeed always divisible by 3.
But really $p = (X-1)X(X+1)$; one of three consecutive numbers will always be divisible by 3. Therefore, for any m, we can take

$$p = (X+1)\cdots(X+m);$$

this will always be divisible by m. Therefore, $d \leqslant m$.

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.
- $X = 1$ gives $1 + a + b \equiv 0 \mod 4 \implies a + b \equiv -1 \mod 4$.
- $X = 2$ gives $8 + 4a + 2b \equiv 0 \mod 4 \implies 2b \equiv 0 \mod 4$.
- $X = -1$ gives $-1 + a - b \equiv 0 \mod 4 \implies a - b \equiv 1 \mod 4$.

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.
- $X = 1$ gives $1 + a + b \equiv 0 \mod 4 \implies a + b \equiv -1 \mod 4$.
- $X = 2$ gives $8 + 4a + 2b \equiv 0 \mod 4 \implies 2b \equiv 0 \mod 4$.
- $X = -1$ gives $-1 + a - b \equiv 0 \mod 4 \implies a - b \equiv 1 \mod 4$.

The second and fourth give $2b \equiv 2 \mod 4$. This contradicts the third, so the answer is *no*. Therefore, $d = 4$.

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.
- $X = 1$ gives $1 + a + b \equiv 0 \mod 4 \implies a + b \equiv -1 \mod 4$.
- $X = 2$ gives $8 + 4a + 2b \equiv 0 \mod 4 \implies 2b \equiv 0 \mod 4$.
- $X = -1$ gives $-1 + a - b \equiv 0 \mod 4 \implies a - b \equiv 1 \mod 4$.

The second and fourth give $2b \equiv 2 \mod 4$. This contradicts the third, so the answer is *no*. Therefore, $d = 4$.

Let $m = 5$. This is prime, so the polynomial

$$\overline{p} \in \mathbb{F}_5[X]$$

can only have d zeroes. It should have 5 zeroes, so $d = 5$ again.

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.
- $X = 1$ gives $1 + a + b \equiv 0 \mod 4 \implies a + b \equiv -1 \mod 4$.
- $X = 2$ gives $8 + 4a + 2b \equiv 0 \mod 4 \implies 2b \equiv 0 \mod 4$.
- $X = -1$ gives $-1 + a - b \equiv 0 \mod 4 \implies a - b \equiv 1 \mod 4$.

The second and fourth give $2b \equiv 2 \mod 4$. This contradicts the third, so the answer is *no*. Therefore, $d = 4$.
Let $m = 5$. This is prime, so the polynomial

$$\overline{p} \in \mathbb{F}_5[X]$$

can only have d zeroes. It should have 5 zeroes, so $d = 5$ again.
So is m is prime, we must have $d = m$. Does this always hold?

Problem I (3/4)

Can $X^3 + aX^2 + bX + c$ always be divisible by 4?

- $X = 0$ gives $c \equiv 0 \mod 4$, so let's say $c = 0$.
- $X = 1$ gives $1 + a + b \equiv 0 \mod 4 \implies a + b \equiv -1 \mod 4$.
- $X = 2$ gives $8 + 4a + 2b \equiv 0 \mod 4 \implies 2b \equiv 0 \mod 4$.
- $X = -1$ gives $-1 + a - b \equiv 0 \mod 4 \implies a - b \equiv 1 \mod 4$.

The second and fourth give $2b \equiv 2 \mod 4$. This contradicts the third, so the answer is *no*. Therefore, $d = 4$.
Let $m = 5$. This is prime, so the polynomial

$$\overline{p} \in \mathbb{F}_5[X]$$

can only have d zeroes. It should have 5 zeroes, so $d = 5$ again.
So is m is prime, we must have $d = m$. Does this always hold?
Look back at $p = (X-1)X(X+1)$. This is always divisible by 3, but also by 2. Therefore, for $m = 6$, we have $d = 3$...

Problem I (4/4)

Are the polynomials $p = (X+1)\cdots(X+d)$ sometimes *better* than "just" divisible by d? Yes!

Problem I (4/4)

Are the polynomials $p = (X+1)\cdots(X+d)$ sometimes *better* than "just" divisible by d? Yes!

Lemma

For any $n \in \mathbb{Z}$, the product $(n+1)\cdots(n+d)$ is divisible by $d!$.

Problem I (4/4)

Are the polynomials $p = (X+1)\cdots(X+d)$ sometimes *better* than "just" divisible by d? Yes!

Lemma

For any $n \in \mathbb{Z}$, the product $(n+1)\cdots(n+d)$ is divisible by $d!$.

Proof.

Indeed, note that

$$\frac{(n+1)\cdots(n+d)}{d!} = \frac{(n+d)!}{n!d!} = \binom{n+d}{d} \in \mathbb{Z},$$

proving the claim. □

Problem I (4/4)

Are the polynomials $p = (X+1)\cdots(X+d)$ sometimes *better* than "just" divisible by d? Yes!

Lemma

For any $n \in \mathbb{Z}$, the product $(n+1)\cdots(n+d)$ is divisible by $d!$.

Proof.

Indeed, note that

$$\frac{(n+1)\cdots(n+d)}{d!} = \frac{(n+d)!}{n!d!} = \binom{n+d}{d} \in \mathbb{Z},$$

proving the claim. □

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Problem II (1/3)

Question

Let G be an abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Problem II (1/3)

Question

Let G be an abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Answer: *no*.

Problem II (1/3)

Question

Let G be an abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Answer: *no*.

Definition

Let $G_1, G_2, \ldots$ be a sequence of abelian groups. Then define the *direct sum* G of these groups as the set

$$G = \bigoplus_{n=1}^{\infty} G_n = \{(g_1, g_2, \ldots) \mid g_n = 0 \text{ for all but finitely many } n\},$$

with coordinate-wise addition.

Problem II (2/3)

Consider the group

$$G = \bigoplus_{n=1}^{\infty} \mathbb{Z}/3^n\mathbb{Z}.$$

Let $f : G \to G$ be given by "multiplication by 1/2", i.e. $2f(g) = g$ for all $g \in G$.

Problem II (2/3)

Consider the group

$$G = \bigoplus_{n=1}^{\infty} \mathbb{Z}/3^n\mathbb{Z}.$$

Let $f : G \to G$ be given by "multiplication by 1/2", i.e. $2f(g) = g$ for all $g \in G$. On each component,

$$\mathbb{Z}/3^n\mathbb{Z} \to \mathbb{Z}/3^n\mathbb{Z} : g \mapsto \frac{3^n + 1}{2} g.$$

Clearly f is not multiplication by a fixed $k \in \mathbb{Z}$.

Problem II (2/3)

Consider the group

$$G = \bigoplus_{n=1}^{\infty} \mathbb{Z}/3^n\mathbb{Z}.$$

Let $f : G \to G$ be given by "multiplication by 1/2", i.e. $2f(g) = g$ for all $g \in G$. On each component,

$$\mathbb{Z}/3^n\mathbb{Z} \to \mathbb{Z}/3^n\mathbb{Z} : g \mapsto \frac{3^n + 1}{2} g.$$

Clearly f is not multiplication by a fixed $k \in \mathbb{Z}$. However, if $g \in G$, then

$$g = (g_1, g_2, \ldots, g_n, 0, 0, \ldots)$$

for some $n \in \mathbb{N}$. Then

$$f(g) = \frac{3^n + 1}{2} g.$$

Therefore we have found a counter-example.

Problem II (3/3)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Problem II (3/3)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Theorem

Let G be a finitely generated abelian group. Then

$$G \cong T \times \mathbb{Z}^n$$

for some finite abelian group T and $n \in \mathbb{N}$.

Problem II (3/3)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Theorem

Let G be a finitely generated abelian group. Then

$$G \cong T \times \mathbb{Z}^n$$

for some finite abelian group T and $n \in \mathbb{N}$.

Suppose G is generated by one element g. Then every $f : G \to G$ is mult. by some fixed $k \in \mathbb{Z}$. Indeed, if $f(g) = kg$, then k always works.

Problem II (3/3)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Theorem

Let G be a finitely generated abelian group. Then

$$G \cong T \times \mathbb{Z}^n$$

for some finite abelian group T and $n \in \mathbb{N}$.

Suppose G is generated by one element g. Then every $f : G \to G$ is mult. by some fixed $k \in \mathbb{Z}$. Indeed, if $f(g) = kg$, then k always works. But what about 2 generators? Or more?

Problem III (1/3)

The Collatz Conjecture

Define a function $f : \mathbb{N} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 3n+1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

Does the sequence $n, f(n), f(f(n)), \ldots$ always eventually reach 1?

Problem III (1/3)

The Collatz Conjecture

Define a function $f : \mathbb{N} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 3n+1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

Does the sequence $n, f(n), f(f(n)), \ldots$ always eventually reach 1?

Famously difficult open problem. I won't claim to be able to solve it.

Problem III (1/3)

The Collatz Conjecture

Define a function $f : \mathbb{N} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 3n + 1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

Does the sequence $n, f(n), f(f(n)), \ldots$ always eventually reach 1?

Famously difficult open problem. I won't claim to be able to solve it.

Question

Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - 1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

When does the sequence $n, f(n), f(f(n)), \ldots$ ever reach the number 1?

Problem III (2/3)

Remark 1

If n is odd, then $n^2 \equiv 1 \mod 8$.
Fix $t \in \mathbb{Z}$ odd. Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - t & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

Problem III (2/3)

Remark 1

If n is odd, then $n^2 \equiv 1 \mod 8$.
Fix $t \in \mathbb{Z}$ odd. Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - t & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

If $t \not\equiv 1 \mod 8$, then $n^2 - t \in \{2, 4, 6\} \mod 8$, so we only divide by 2 at most once or twice. So as soon as $n^2 - t > 4n$, the sequence grows forever - not very interesting.

Problem III (2/3)

Remark 1

If n is odd, then $n^2 \equiv 1 \mod 8$.
Fix $t \in \mathbb{Z}$ odd. Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - t & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

If $t \not\equiv 1 \mod 8$, then $n^2 - t \in \{2, 4, 6\} \mod 8$, so we only divide by 2 at most once or twice. So as soon as $n^2 - t > 4n$, the sequence grows forever - not very interesting.

Remark 2

I proposed the $t = -3$ case to the Dutch mathematics olympiad; then only $1 \to 4 \to 2 \to 1$ and $3 \to 12 \to 6 \to 3$ do not explode. It was selected; a great problem for smart high schoolers :)

Problem III (3/3)

$3 \mapsto 8 \mapsto 4 \mapsto 2 \mapsto 1$

$5 \mapsto 24 \mapsto 12 \mapsto 6 \mapsto 3$

$7 \mapsto 48 \mapsto 24$

$9 \mapsto 80 \mapsto 40 \mapsto 20 \mapsto 10 \mapsto 5$

$11 \mapsto 120 \mapsto 60 \mapsto 30 \mapsto 15 \mapsto 224 \mapsto 112 \mapsto 56 \mapsto 28 \mapsto 14 \mapsto 7$

$13 \mapsto 168 \mapsto 84 \mapsto 42 \mapsto 21 \mapsto 440 \mapsto 220 \mapsto 110 \mapsto 55 \mapsto 3024 \mapsto \ldots$

$17 \mapsto 288 \mapsto 144 \mapsto 72 \mapsto 36 \mapsto 18 \mapsto 9$

$19 \mapsto 360 \mapsto 180 \mapsto 90 \mapsto 45 \mapsto 2024 \mapsto 1012 \mapsto 506 \mapsto 253 \mapsto \ldots$

$23 \mapsto 528 \mapsto 264 \mapsto 132 \mapsto 66 \mapsto 33 \mapsto 1088 \mapsto 544 \mapsto 272 \mapsto 136 \mapsto 68 \mapsto 34 \mapsto 17$

Problem III (3/3)

$3 \mapsto 8 \mapsto 4 \mapsto 2 \mapsto 1$

$5 \mapsto 24 \mapsto 12 \mapsto 6 \mapsto 3$

$7 \mapsto 48 \mapsto 24$

$9 \mapsto 80 \mapsto 40 \mapsto 20 \mapsto 10 \mapsto 5$

$11 \mapsto 120 \mapsto 60 \mapsto 30 \mapsto 15 \mapsto 224 \mapsto 112 \mapsto 56 \mapsto 28 \mapsto 14 \mapsto 7$

$13 \mapsto 168 \mapsto 84 \mapsto 42 \mapsto 21 \mapsto 440 \mapsto 220 \mapsto 110 \mapsto 55 \mapsto 3024 \mapsto \dots$

$17 \mapsto 288 \mapsto 144 \mapsto 72 \mapsto 36 \mapsto 18 \mapsto 9$

$19 \mapsto 360 \mapsto 180 \mapsto 90 \mapsto 45 \mapsto 2024 \mapsto 1012 \mapsto 506 \mapsto 253 \mapsto \dots$

$23 \mapsto 528 \mapsto 264 \mapsto 132 \mapsto 66 \mapsto 33 \mapsto 1088 \mapsto 544 \mapsto 272 \mapsto 136 \mapsto$
$68 \mapsto 34 \mapsto 17$

Remark

Since $n^2 - 1 = (n-1)(n+1)$, if we have $n = 2^k \pm 1$, then $f(n) = 2^{k+1} \cdot (2^{k-1} \pm 1)$, so by induction these numbers will always go down to 1. But this does not explain 11 or 23...

Part 2: Solutions

Solution I (1/2)

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Solution I (1/2)

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Definition

Let $p \in \mathbb{Q}[X]$ be any polynomial. Then define its *discrete derivative* by

$$(\Delta p)(X) = p(X+1) - p(X).$$

Solution I (1/2)

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Definition

Let $p \in \mathbb{Q}[X]$ be any polynomial. Then define its *discrete derivative* by

$$(\Delta p)(X) = p(X+1) - p(X).$$

Lemma

Let $p \in \mathbb{Q}[X]$ be of degree d. Then:

- The degree of Δp is precisely $d-1$;

Solution I (1/2)

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Definition

Let $p \in \mathbb{Q}[X]$ be any polynomial. Then define its *discrete derivative* by

$$(\Delta p)(X) = p(X+1) - p(X).$$

Lemma

Let $p \in \mathbb{Q}[X]$ be of degree d. Then:

- The degree of Δp is precisely $d-1$;
- If $p(n)$ is an integer for all $n \in \mathbb{Z}$, then so is $(\Delta p)(n)$.

Solution I (1/2)

Conjecture

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Definition

Let $p \in \mathbb{Q}[X]$ be any polynomial. Then define its *discrete derivative* by

$$(\Delta p)(X) = p(X+1) - p(X).$$

Lemma

Let $p \in \mathbb{Q}[X]$ be of degree d. Then:

- The degree of Δp is precisely $d-1$;
- If $p(n)$ is an integer for all $n \in \mathbb{Z}$, then so is $(\Delta p)(n)$.
- The leading coefficient of Δp is precisely d times that of p.

The first two are trivial, and indeed $(X+1)^d - X^d = dX^{d-1} + \ldots$.

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Proof.

Let $p \in \mathbb{Z}[X]$ be any polynomial with $m \mid p(n)$ for all $n \in \mathbb{Z}$ and let d denote its degree. Then the polynomial $P = p/m \in \mathbb{Q}[X]$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Proof.

Let $p \in \mathbb{Z}[X]$ be any polynomial with $m \mid p(n)$ for all $n \in \mathbb{Z}$ and let d denote its degree. Then the polynomial $P = p/m \in \mathbb{Q}[X]$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Now consider $\Delta^d P$. Then:

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Proof.

Let $p \in \mathbb{Z}[X]$ be any polynomial with $m \mid p(n)$ for all $n \in \mathbb{Z}$ and let d denote its degree. Then the polynomial $P = p/m \in \mathbb{Q}[X]$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Now consider $\Delta^d P$. Then:

- Since the degree drops by 1 for each application of Δ, the degree of $\Delta^d P$ is zero. In other words, it is constant.

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Proof.

Let $p \in \mathbb{Z}[X]$ be any polynomial with $m \mid p(n)$ for all $n \in \mathbb{Z}$ and let d denote its degree. Then the polynomial $P = p/m \in \mathbb{Q}[X]$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Now consider $\Delta^d P$. Then:

- Since the degree drops by 1 for each application of Δ, the degree of $\Delta^d P$ is zero. In other words, it is constant.
- Its leading coefficient is first multiplied by d, then by $d-1$, then by $d-2$, etc. We started with $1/m$, so we end up with $d!/m$.

Solution I (2/2)

Theorem

Let $m \in \mathbb{N}$. There exists a polynomial of degree d such that $m \mid p(n)$ for all $n \in \mathbb{Z}$ if and only if $m \mid d!$.

Proof.

Let $p \in \mathbb{Z}[X]$ be any polynomial with $m \mid p(n)$ for all $n \in \mathbb{Z}$ and let d denote its degree. Then the polynomial $P = p/m \in \mathbb{Q}[X]$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Now consider $\Delta^d P$. Then:

- Since the degree drops by 1 for each application of Δ, the degree of $\Delta^d P$ is zero. In other words, it is constant.
- Its leading coefficient is first multiplied by d, then by $d-1$, then by $d-2$, etc. We started with $1/m$, so we end up with $d!/m$.
- $(\Delta^d P)(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$, because this was true for P, and Δ conserves this property.

In other words, $\Delta^d P = d!/m \in \mathbb{Z}$. □

Solution II (1/4)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

Solution II (1/4)

Question

Let G be a *finitely generated* abelian group and let $f : G \to G$ be a group endomorphism. Suppose that for each $g \in G$, there exists some integer $k_g \in \mathbb{Z}$ such that $f(g) = k_g g$. Does there necessarily exist some $k \in \mathbb{Z}$ such that $f(g) = kg$ for all $g \in G$?

We will proceed by induction on the number of generators of G.

Two generators (1/2)

If G has two generators, then either

$$G \cong C_n \times C_m, \quad G \cong \mathbb{Z} \times C_n, \quad \text{or} \quad G \cong \mathbb{Z} \times \mathbb{Z}.$$

In any case, we can find $a, b \in G$ such that

$$\langle a, b \rangle = G \quad \text{and} \quad \langle a \rangle \cap \langle b \rangle = \{0\}.$$

Solution II (2/4)

Two generators (2/2)

So take $a, b \in G$ such that

$$\langle a, b \rangle = G \quad \text{and} \quad \langle a \rangle \cap \langle b \rangle = \{0\}.$$

By assumption, there exist $x, y, z \in \mathbb{Z}$ such that

$$f(a) = xa, \quad f(b) = yb \quad \text{and} \quad f(a+b) = z(a+b).$$

Solution II (2/4)

Two generators (2/2)

So take $a, b \in G$ such that

$$\langle a, b \rangle = G \quad \text{and} \quad \langle a \rangle \cap \langle b \rangle = \{0\}.$$

By assumption, there exist $x, y, z \in \mathbb{Z}$ such that

$$f(a) = xa, \quad f(b) = yb \quad \text{and} \quad f(a+b) = z(a+b).$$

But then

$$0 = f(a+b) - f(a) - f(b) = (z-x)a + (z-y)b.$$

Solution II (2/4)

Two generators (2/2)

So take $a, b \in G$ such that

$$\langle a, b\rangle = G \quad \text{and} \quad \langle a\rangle \cap \langle b\rangle = \{0\}.$$

By assumption, there exist $x, y, z \in \mathbb{Z}$ such that

$$f(a) = xa, \quad f(b) = yb \quad \text{and} \quad f(a+b) = z(a+b).$$

But then

$$0 = f(a+b) - f(a) - f(b) = (z-x)a + (z-y)b.$$

Since $\langle a\rangle \cap \langle b\rangle = \{0\}$, it thus follows that

$$(z-x)a = 0 \quad \text{and} \quad (z-y)b = 0 \implies xa = za \quad \text{and} \quad yb = zb.$$

Solution II (2/4)

Two generators (2/2)

So take $a, b \in G$ such that

$$\langle a, b\rangle = G \quad \text{and} \quad \langle a\rangle \cap \langle b\rangle = \{0\}.$$

By assumption, there exist $x, y, z \in \mathbb{Z}$ such that

$$f(a) = xa, \quad f(b) = yb \quad \text{and} \quad f(a+b) = z(a+b).$$

But then

$$0 = f(a+b) - f(a) - f(b) = (z-x)a + (z-y)b.$$

Since $\langle a\rangle \cap \langle b\rangle = \{0\}$, it thus follows that

$$(z-x)a = 0 \quad \text{and} \quad (z-y)b = 0 \implies xa = za \quad \text{and} \quad yb = zb.$$

Therefore $f(a) = za$ and $f(b) = zb$, so f is mult. by z on all of G. □

Solution II (3/4)

Induction step

Now let G be an abelian group on $n \geqslant 3$ generators, say $G = \langle a_1, \ldots, a_n \rangle$. Then consider the subgroups

$$H_1 = \langle a_1, a_n \rangle, \quad H_2 = \langle a_1, \ldots, a_{n-1} \rangle, \quad H_3 = \langle a_2, \ldots, a_n \rangle.$$

Solution II (3/4)

Induction step

Now let G be an abelian group on $n \geqslant 3$ generators, say $G = \langle a_1, \dots, a_n \rangle$. Then consider the subgroups

$$H_1 = \langle a_1, a_n \rangle, \quad H_2 = \langle a_1, \dots, a_{n-1} \rangle, \quad H_3 = \langle a_2, \dots, a_n \rangle.$$

By the induction hypothesis, the map $f : G \to G$ will be given by multiplication by some fixed integers k_i on H_i for $i \in \{1, 2, 3\}$.

Solution II (3/4)

Induction step

Now let G be an abelian group on $n \geqslant 3$ generators, say $G = \langle a_1, \dots, a_n \rangle$. Then consider the subgroups

$$H_1 = \langle a_1, a_n \rangle, \quad H_2 = \langle a_1, \dots, a_{n-1} \rangle, \quad H_3 = \langle a_2, \dots, a_n \rangle.$$

By the induction hypothesis, the map $f : G \to G$ will be given by multiplication by some fixed integers k_i on H_i for $i \in \{1, 2, 3\}$. For $i, j \in \{1, 2, 3\}$, this means that on $H_i \cap H_j$, multiplication by k_i and k_j is the same. Therefore $(k_i - k_j)(H_i \cap H_j) = 0$,

Induction step

Now let G be an abelian group on $n \geqslant 3$ generators, say $G = \langle a_1, \dots, a_n \rangle$. Then consider the subgroups

$$H_1 = \langle a_1, a_n \rangle, \quad H_2 = \langle a_1, \dots, a_{n-1} \rangle, \quad H_3 = \langle a_2, \dots, a_n \rangle.$$

By the induction hypothesis, the map $f : G \to G$ will be given by multiplication by some fixed integers k_i on H_i for $i \in \{1, 2, 3\}$. For $i, j \in \{1, 2, 3\}$, this means that on $H_i \cap H_j$, multiplication by k_i and k_j is the same. Therefore $(k_i - k_j)(H_i \cap H_j) = 0$, and f on $H_i \cap H_j$ can be described as multiplication by any number in the arithmetic progression

$$A_{ij} = \{k_j + (k_i - k_j)m \mid m \in \mathbb{Z}\}.$$

Solution II (3/4)

Induction step

Now let G be an abelian group on $n \geqslant 3$ generators, say $G = \langle a_1, \ldots, a_n \rangle$. Then consider the subgroups

$$H_1 = \langle a_1, a_n \rangle, \quad H_2 = \langle a_1, \ldots, a_{n-1} \rangle, \quad H_3 = \langle a_2, \ldots, a_n \rangle.$$

By the induction hypothesis, the map $f : G \to G$ will be given by multiplication by some fixed integers k_i on H_i for $i \in \{1, 2, 3\}$. For $i, j \in \{1, 2, 3\}$, this means that on $H_i \cap H_j$, multiplication by k_i and k_j is the same. Therefore $(k_i - k_j)(H_i \cap H_j) = 0$, and f on $H_i \cap H_j$ can be described as multiplication by any number in the arithmetic progression

$$A_{ij} = \{k_j + (k_i - k_j)m \mid m \in \mathbb{Z}\}.$$

Do these arithmetic progressions all have a number in common?

Solution II (4/4)

Proposition

Consider three arithmetic progressions inside $\mathbb{Z}$. Suppose that pairwise they have a number in common. Then all three of them have a number in common.

Solution II (4/4)

Proposition

Consider three arithmetic progressions inside $\mathbb{Z}$. Suppose that pairwise they have a number in common. Then all three of them have a number in common.

I will leave the proof as an exercise :)

Solution II (4/4)

Proposition

Consider three arithmetic progressions inside $\mathbb{Z}$. Suppose that pairwise they have a number in common. Then all three of them have a number in common.

I will leave the proof as an exercise :)

Completing the proof

Note that the arithmetic progressions $A_{ij} = \{k_j + (k_i - k_j)m \mid m \in \mathbb{Z}\}$ contain by construction both the numbers k_i and k_j. Therefore, A_{12}, A_{23} and A_{31} pairwise have a number in common. It follows that all three share some number k.

Solution II (4/4)

Proposition

Consider three arithmetic progressions inside $\mathbb{Z}$. Suppose that pairwise they have a number in common. Then all three of them have a number in common.

I will leave the proof as an exercise :)

Completing the proof

Note that the arithmetic progressions $A_{ij} = \{k_j + (k_i - k_j)m \mid m \in \mathbb{Z}\}$ contain by construction both the numbers k_i and k_j. Therefore, A_{12}, A_{23} and A_{31} pairwise have a number in common. It follows that all three share some number k. By definition, this means that f on each of

$$a_1 \in (H_1 \cap H_2) \quad a_2, \ldots, a_{n-1} \in (H_2 \cap H_3) \quad \text{and} \quad a_n \in (H_3 \cap H_1)$$

is given by multiplication by k.

Solution II (4/4)

Proposition

Consider three arithmetic progressions inside $\mathbb{Z}$. Suppose that pairwise they have a number in common. Then all three of them have a number in common.

I will leave the proof as an exercise :)

Completing the proof

Note that the arithmetic progressions $A_{ij} = \{k_j + (k_i - k_j)m \mid m \in \mathbb{Z}\}$ contain by construction both the numbers k_i and k_j. Therefore, A_{12}, A_{23} and A_{31} pairwise have a number in common. It follows that all three share some number k. By definition, this means that f on each of

$$a_1 \in (H_1 \cap H_2) \quad a_2, \ldots, a_{n-1} \in (H_2 \cap H_3) \quad \text{and} \quad a_n \in (H_3 \cap H_1)$$

is given by multiplication by k. This shows $f(a_i) = ka_i$ for all generators a_i of G, so f is multiplication by k on all of G. □

Solution III (1/4)

Question

Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - 1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

When does the sequence $n, f(n), f(f(n)), \ldots$ ever reach the number 1?

Solution III (1/4)

Question

Define a function $f : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by

$$f(n) = \begin{cases} n^2 - 1 & \text{if } n \text{ is odd;} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

When does the sequence $n, f(n), f(f(n)), \ldots$ ever reach the number 1?

Let's make our lives a little bit easier:

Question

Define a function $g : \mathbb{N}_{\text{odd}} \setminus \{1\} \to \mathbb{N}_{\text{odd}}$ by

$$g(n) = k \quad \text{where} \quad n^2 - 1 = 2^m \cdot k \quad \text{with } k \text{ odd.}$$

When does the sequence $n, g(n), g(g(n)), \ldots$ ever reach the number 1?

Solution III (2/4)

Lemma

It holds that $g(n) < n$ if and only if $n = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Solution III (2/4)

Lemma

It holds that $g(n) < n$ if and only if $n = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

We have seen before that $g(2^t \pm 1) = 2^{t-1} \pm 1$. For other n, one of the factors of $n^2 - 1 = (n+1)(n-1)$ will contain precisely one factor of 2. Since neither is a power of 2 by assumption, after taking away all factors of 2, both will be at least 3.

Solution III (2/4)

Lemma

It holds that $g(n) < n$ if and only if $n = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

We have seen before that $g(2^t \pm 1) = 2^{t-1} \pm 1$. For other n, one of the factors of $n^2 - 1 = (n+1)(n-1)$ will contain precisely one factor of 2. Since neither is a power of 2 by assumption, after taking away all factors of 2, both will be at least 3. Therefore

$$g(n) \geqslant 3 \cdot \frac{n-1}{2} \geqslant n$$

for $n \geqslant 3$, completing the proof. □

Solution III (2/4)

Lemma

It holds that $g(n) < n$ if and only if $n = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

We have seen before that $g(2^t \pm 1) = 2^{t-1} \pm 1$. For other n, one of the factors of $n^2 - 1 = (n+1)(n-1)$ will contain precisely one factor of 2. Since neither is a power of 2 by assumption, after taking away all factors of 2, both will be at least 3. Therefore

$$g(n) \geqslant 3 \cdot \frac{n-1}{2} \geqslant n$$

for $n \geqslant 3$, completing the proof. □

Any sequence $n, g(n), g(g(n)), \ldots$ that ever ends at 1, must go down at some point. Therefore, some number of the form $2^t \pm 1$ must appear in the sequence. We therefore reduce to solving $g(n) = 2^t \pm 1$.

Solution III (3/4)

Proposition

The odd positive integers n for which $g(n) = 2^t \pm 1$ for some $t \in \mathbb{N}$ are precisely those $2^t \pm 1$ themselves, and additionally the three exceptional solutions $n = 11$, $n = 23$ and $n = 181$.

Solution III (3/4)

Proposition

The odd positive integers n for which $g(n) = 2^t \pm 1$ for some $t \in \mathbb{N}$ are precisely those $2^t \pm 1$ themselves, and additionally the three exceptional solutions $n = 11$, $n = 23$ and $n = 181$.

Proof.

We must find all solutions to the equations

$$n^2 - 1 = (2^t \pm 1) \cdot 2^m \iff n^2 = 2^{t+m} \pm 2^m + 1.$$

Solution III (3/4)

Proposition

The odd positive integers n for which $g(n) = 2^t \pm 1$ for some $t \in \mathbb{N}$ are precisely those $2^t \pm 1$ themselves, and additionally the three exceptional solutions $n = 11$, $n = 23$ and $n = 181$.

Proof.

We must find all solutions to the equations

$$n^2 - 1 = (2^t \pm 1) \cdot 2^m \iff n^2 = 2^{t+m} \pm 2^m + 1.$$

Fortunately, we may appeal to the 2002 article “The equations $2^n \pm 2^m \pm 2^l = z^2$” by László Szalay and claim the result. □

Solution III (3/4)

Proposition

The odd positive integers n for which $g(n) = 2^t \pm 1$ for some $t \in \mathbb{N}$ are precisely those $2^t \pm 1$ themselves, and additionally the three exceptional solutions $n = 11$, $n = 23$ and $n = 181$.

Proof.

We must find all solutions to the equations

$$n^2 - 1 = (2^t \pm 1) \cdot 2^m \iff n^2 = 2^{t+m} \pm 2^m + 1.$$

Fortunately, we may appeal to the 2002 article "The equations $2^n \pm 2^m \pm 2^l = z^2$" by László Szalay and claim the result. □

So, we reduce to finding all n such that

$$g(n) \in \{11, 23, 181\}.$$

Note that all of these are prime.

Solution III (4/4)

Lemma

If $g(n) = p$ is prime, then $p = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Solution III (4/4)

Lemma

If $g(n) = p$ is prime, then $p = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

If $g(n) = p$ is prime, then

$$(n-1)(n+1) = p \cdot 2^m.$$

But one of $n-1$ and $n+1$ will contain precisely one factor of 2.

Solution III (4/4)

Lemma

If $g(n) = p$ is prime, then $p = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

If $g(n) = p$ is prime, then

$$(n-1)(n+1) = p \cdot 2^m.$$

But one of $n-1$ and $n+1$ will contain precisely one factor of 2. Therefore, one is either 2, yielding $n \in \{1, 3\}$, or $2p$, yielding $(n-1)(n+1) = 2p(2p \pm 2)$. But then $p \pm 1 = 2^{m-2}$. □

The remaining values 11, 23 and 181 are not of this form, so:

Solution III (4/4)

Lemma

If $g(n) = p$ is prime, then $p = 2^t \pm 1$ for some $t \in \mathbb{N}$.

Proof.

If $g(n) = p$ is prime, then

$$(n-1)(n+1) = p \cdot 2^m.$$

But one of $n-1$ and $n+1$ will contain precisely one factor of 2. Therefore, one is either 2, yielding $n \in \{1,3\}$, or $2p$, yielding $(n-1)(n+1) = 2p(2p \pm 2)$. But then $p \pm 1 = 2^{m-2}$. □

The remaining values 11, 23 and 181 are not of this form, so:

Theorem

The only odd numbers for which the sequence $n, f(n), f(f(n)), \ldots$ eventually reaches 1 are precisely all numbers of the form $2^t \pm 1$ and additionally the exceptional values $n \in \{11, 23, 181\}$.

Thanks for listening!

$$181 \mapsto 16380 \mapsto 8190 \mapsto 4095 \mapsto 16769024 \mapsto 8384512 \mapsto 4192256$$
$$\mapsto 2096128 \mapsto 1048064 \mapsto 524032 \mapsto 262016 \mapsto 131008 \mapsto 65504$$
$$\mapsto 32752 \mapsto 16376 \mapsto 8188 \mapsto 4094 \mapsto 2047 \mapsto 4190208 \mapsto 2095104$$
$$\mapsto 1047552 \mapsto 523776 \mapsto 261888 \mapsto 130944 \mapsto 65472 \mapsto 32736$$
$$\mapsto 16368 \mapsto 8184 \mapsto 4092 \mapsto 2046 \mapsto 1023 \mapsto 1046528 \mapsto 523264$$
$$\mapsto 261632 \mapsto 130816 \mapsto 65408 \mapsto 32704 \mapsto 16352 \mapsto 8176 \mapsto 4088$$
$$\mapsto 2044 \mapsto 1022 \mapsto 511 \mapsto 261120 \mapsto 130560 \mapsto 65280 \mapsto 32640$$
$$\mapsto 16320 \mapsto 8160 \mapsto 4080 \mapsto 2040 \mapsto 1020 \mapsto 510 \mapsto 255 \mapsto 65024$$
$$\mapsto 32512 \mapsto 16256 \mapsto 8128 \mapsto 4064 \mapsto 2032 \mapsto 1016 \mapsto 508 \mapsto 254$$
$$\mapsto 127 \mapsto 16128 \mapsto 8064 \mapsto 4032 \mapsto 2016 \mapsto 1008 \mapsto 504 \mapsto 252$$
$$\mapsto 126 \mapsto 63 \mapsto 3968 \mapsto 1984 \mapsto 992 \mapsto 496 \mapsto 248 \mapsto 124 \mapsto 62$$
$$\mapsto 31 \mapsto 960 \mapsto 480 \mapsto 240 \mapsto 120 \mapsto 60 \mapsto 30 \mapsto 15 \mapsto 224 \mapsto 112$$
$$\mapsto 56 \mapsto 28 \mapsto 14 \mapsto 7 \mapsto 48 \mapsto 24 \mapsto 12 \mapsto 6 \mapsto 3 \mapsto 8 \mapsto 4 \mapsto 2 \mapsto 1.$$