The Skolem Problem: a century-old enigma at the heart of computation

Joël Ouaknine

Max Planck Institute for Software Systems, Germany

SIC Lecture Series October
4 February 2026

Funded by the European Union
erc European Research Council
DynAMiCs
Funded by DFG Deutsche Forschungsgemeinschaft German Research Foundation

"Prediction is very difficult, especially about the future"

Niels Bohr

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u';\ v := v';\ w := w';$

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u'; v := v'; w := w';$

1
16
12
34
128
−34
792
−406
2848
1006
2472
26554
−35632
175646
−192648
555914
66688

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u'; v := v'; w := w';$

1	−392114
16	6543432
12	−13596326
34	42901808
128	−61158274
−34	115058712
792	15425834
−406	−297258272
2848	1791381166
1006	−4320278808
2472	11042118394
26554	−17131261552
−35632	24186090206
175646	10655218872
−192648	−120064782646
555914	513956123968
66688	−1281554407154

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u'; v := v'; w := w';$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u'; v := v'; w := w';$

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Example: does this loop eventually terminate?

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u';\ v := v';\ w := w';$

SKOLEM PROBLEM

$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Example: does this loop eventually terminate?

$u := 1;$

SKOLEM-COMPLETE

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u';\ v := v';\ w := w';$

SKOLEM PROBLEM

$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

The Skolem Problem: open for nearly a century!

The Skolem Problem (1934)

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Is there some $n \geq 0$ such that $u_n = 0$?

The Skolem Problem: open for nearly a century!

The Skolem Problem (1934)

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Is there some $n \geq 0$ such that $u_n = 0$?

"It is faintly outrageous that this problem is still open"

Terence Tao, 2007

The Skolem Problem: open for nearly a century!

The Skolem Problem (1934)

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$

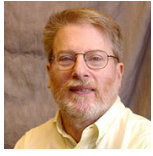
Question: Is there some $n \geq 0$ such that $u_n = 0$?

"It is faintly outrageous that this problem is still open"

Terence Tao, 2007

"Arguably, by some distance, the most prominent problem whose decidability status is currently unknown"

Richard Lipton, 2022



The Skolem Problem: open for nearly a century!

The Skolem Problem (1934)

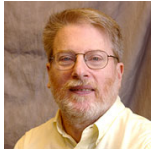
Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Is there some $n \geq 0$ such that $u_n = 0$?

"It is faintly outrageous that this problem is still open"

Terence Tao, 2007

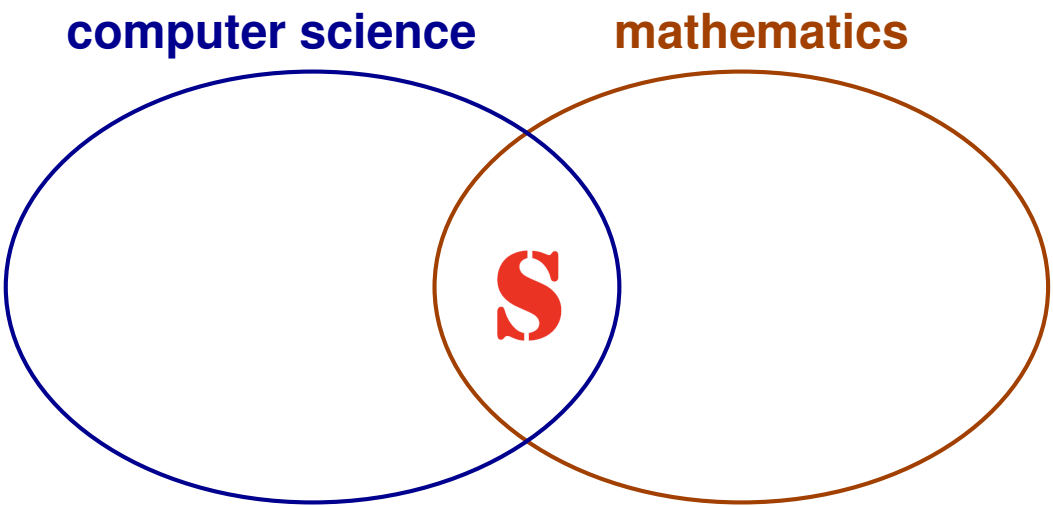
"Arguably, by some distance, the most prominent problem whose decidability status is currently unknown"

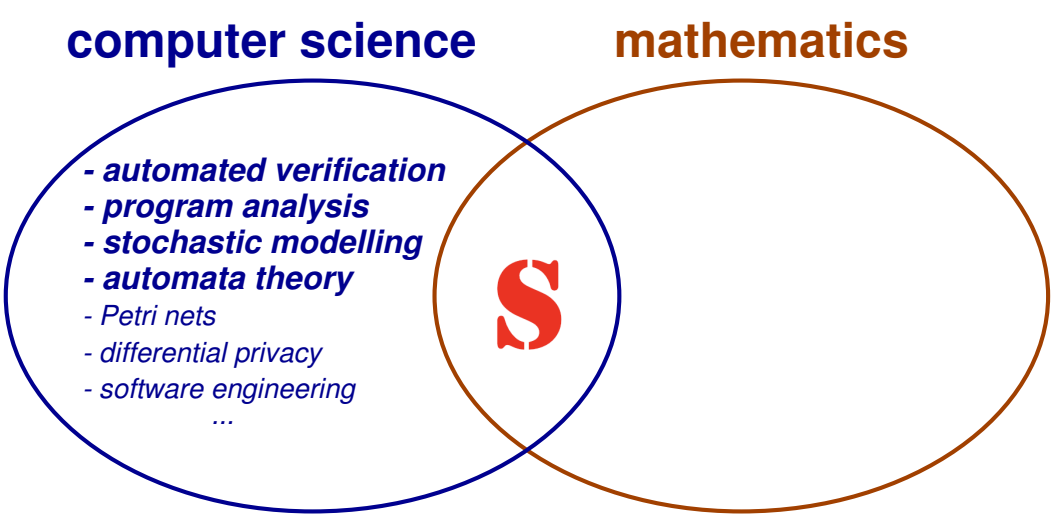
Richard Lipton, 2022

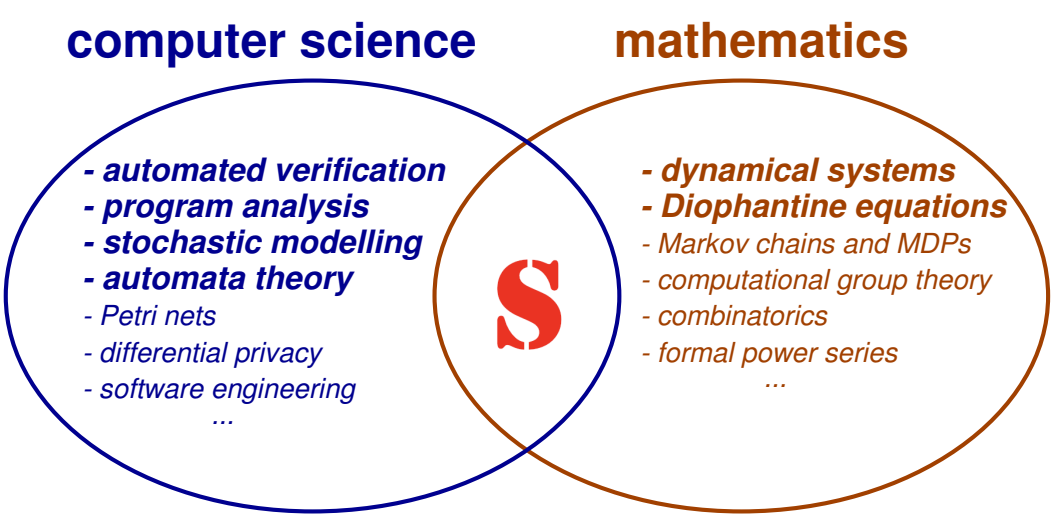


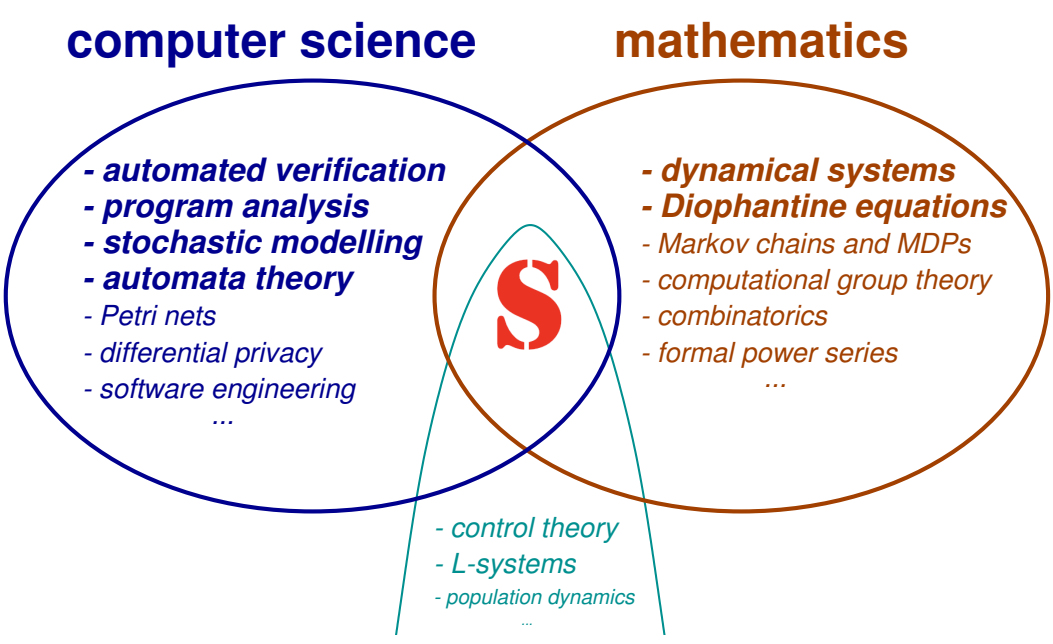
"Some obscure problem that Joël is working on"

Peter Druschel, 2026


computer science
mathematics
S


computer science
mathematics
- automated verification
- program analysis
- stochastic modelling
- automata theory
- Petri nets
- differential privacy
- software engineering
...
S

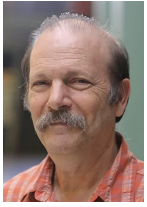

computer science
- automated verification
- program analysis
- stochastic modelling
- automata theory
- Petri nets
- differential privacy
- software engineering
...
S
mathematics
- dynamical systems
- Diophantine equations
- Markov chains and MDPs
- computational group theory
- combinatorics
- formal power series
...


computer science
mathematics
- automated verification
- program analysis
- stochastic modelling
- automata theory
- Petri nets
- differential privacy
- software engineering
...
- dynamical systems
- Diophantine equations
- Markov chains and MDPs
- computational group theory
- combinatorics
- formal power series
...
S
- control theory
- L-systems
- population dynamics
...

The Exponential-Bound Problem (EBP)

From *Sequentical Relational Decomposition*
(Fried, Legay, O., Vardi), LICS'18, LMCS'22

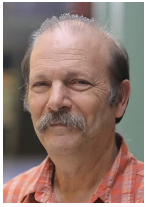
Given a regular language L over a finite alphabet Σ,
for each n, let L_n be the set of words in L of length n



The Exponential-Bound Problem (EBP)

From *Sequentical Relational Decomposition*
(Fried, Legay, O., Vardi), LICS'18, LMCS'22

Given a regular language L over a finite alphabet Σ, for each n, let L_n be the set of words in L of length n



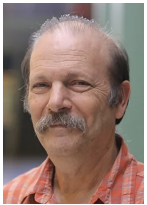
The Exponential-Bound Problem (EBP)

Instance: A regular language L
Question: Is $|L_n| \leq 2^n$ for all n?

The Exponential-Bound Problem (EBP)

From *Sequentical Relational Decomposition*
(Fried, Legay, O., Vardi), LICS'18, LMCS'22

Given a regular language L over a finite alphabet Σ,
for each n, let L_n be the set of words in L of length n



The Exponential-Bound Problem (EBP)

Instance: A regular language L
Question: Is $|L_n| \leq 2^n$ for all n?

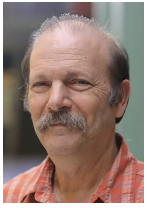
EBP-Reach

Instance: A regular language L
Question: Does $|L_n| = 2^n$ for some n?

The Exponential-Bound Problem (EBP)

From *Sequentical Relational Decomposition*
(Fried, Legay, O., Vardi), LICS'18, LMCS'22

Given a regular language L over a finite alphabet Σ,
for each n, let L_n be the set of words in L of length n



The Exponential-Bound Problem (EBP)

Instance: A regular language L
Question: Is $|L_n| \leq 2^n$ for all n?

EBP-Reach

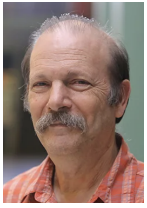
Instance: A regular language L
Question: Does $|L_n| = 2^n$ for some n?

SKOLEM-HARD

The Exponential-Bound Problem (EBP)

From *Sequentical Relational Decomposition*
(Fried, Legay, O., Vardi), LICS'18, LMCS'22

Given a regular language L over a finite alphabet Σ,
for each n, let L_n be the set of words in L of length n



The Exponential-Bound Problem (EBP)

Instance: A regular language L
Question: Is $|L_n| \leq 2^n$ for all n?

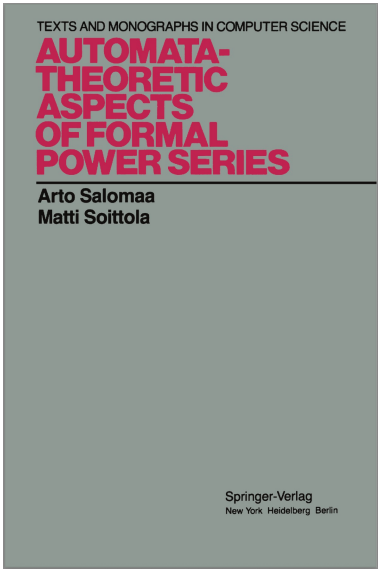
SKOLEM-HARD

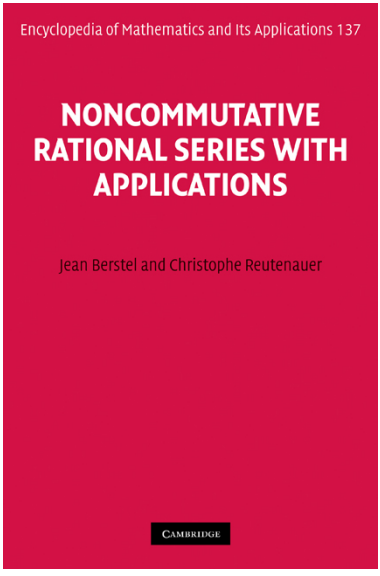
EBP-Reach

Instance: A regular language L
Question: Does $|L_n| = 2^n$ for some n?

SKOLEM-COMPLETE

Rational functions and formal power series





Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Let's assume that $q(0) \neq 0$ (so $f(0)$ is defined)

Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Let's assume that $q(0) \neq 0$ (so $f(0)$ is defined)

Positivity of all derivatives

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) > 0$ for all n?

Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Let's assume that $q(0) \neq 0$ (so $f(0)$ is defined)

Positivity of all derivatives

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) > 0$ for all n?

Vanishing of some derivative

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) = 0$ for some n?

Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Let's assume that $q(0) \neq 0$ (so $f(0)$ is defined)

Positivity of all derivatives

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) > 0$ for all n?

SKOLEM-HARD

Vanishing of some derivative

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) = 0$ for some n?

Rational functions and formal power series

A *rational function* is a ratio of two polynomials: $f(x) = \dfrac{p(x)}{q(x)}$

Let's assume that $q(0) \neq 0$ (so $f(0)$ is defined)

Positivity of all derivatives

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) > 0$ for all n?

SKOLEM-HARD

Vanishing of some derivative

Instance: A rational function $f(x)$
Question: Is $f^{(n)}(0) = 0$ for some n?

SKOLEM-COMPLETE

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

- its first k initial values $u_0, \ldots, u_{k-1}$, and

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

- its first k initial values $u_0, \ldots, u_{k-1}$, and
- its defining recurrence relation: $u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n$

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

- its first k initial values $u_0, \ldots, u_{k-1}$, and
- its defining recurrence relation: $u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n$

The *size* $||\boldsymbol{u}||$ of $\boldsymbol{u}$ is the length of the bit encoding of $(u_0, \ldots, u_{k-1}, a_1, \ldots, a_k)$

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

- its first k initial values $u_0, \ldots, u_{k-1}$, and
- its defining recurrence relation: $u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n$

The *size* $||\boldsymbol{u}||$ of $\boldsymbol{u}$ is the length of the bit encoding of $(u_0, \ldots, u_{k-1}, a_1, \ldots, a_k)$

The Skolem Problem

Instance: An LRS $\boldsymbol{u}$
Question: Is there some $n \geq 0$ such that $u_n = 0$?

The Bounded Skolem Problem

A linear recurrence sequence (LRS) $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ of **order** k is specified by:

- its first k initial values $u_0, \ldots, u_{k-1}$, and
- its defining recurrence relation: $u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n$

The *size* $||\boldsymbol{u}||$ of $\boldsymbol{u}$ is the length of the bit encoding of $(u_0, \ldots, u_{k-1}, a_1, \ldots, a_k)$

The Skolem Problem

Instance: An LRS $\boldsymbol{u}$
Question: Is there some $n \geq 0$ such that $u_n = 0$?

The Bounded Skolem Problem

Instance: An LRS $\boldsymbol{u}$ and a bound B
Question: Is there some $n \in \{0, \ldots, B\}$ such that $u_n = 0$?

The Bounded Skolem Problem: Complexity

$u := 1;$
$v := 2;$
$w := 3;$

while $u \neq 0$ do

$u' := 5u - 2v + 5w;$
$v' := 10u + 3v - 14w;$
$w' := 3v - 10w;$

$u := u'; v := v'; w := w';$

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

The Bounded Skolem Problem: Complexity

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B

Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$
2. using iterated matrix squaring, construct a polynomial-size arithmetic circuit $C(n)$ outputting u_n

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$
2. using iterated matrix squaring, construct a polynomial-size arithmetic circuit $C(n)$ outputting u_n
3. determine if $C(n) = 0$
   (in coRP by [Schönhage 1979])

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$
2. using iterated matrix squaring, construct a polynomial-size arithmetic circuit $C(n)$ outputting u_n
3. determine if $C(n) = 0$ (in coRP by [Schönhage 1979])

Theorem

The Bounded Skolem Problem is in $\mathrm{NP}^{\mathrm{RP}}$.

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$
2. using iterated matrix squaring, construct a polynomial-size arithmetic circuit $C(n)$ outputting u_n
3. determine if $C(n) = 0$ (in coRP by [Schönhage 1979])

Theorem

The Bounded Skolem Problem is in $\mathrm{NP}^{\mathrm{RP}}$.

Theorem (Blondel & Portier 2002)

The Bounded Skolem Problem is NP*-hard.*

The Bounded Skolem Problem: Complexity

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1. guess an index $n \in \{0, \ldots, B\}$
2. using iterated matrix squaring, construct a polynomial-size arithmetic circuit $C(n)$ outputting u_n
3. determine if $C(n) = 0$ (in coRP by [Schönhage 1979])

Theorem

The Bounded Skolem Problem is in $\mathrm{NP}^{\mathrm{RP}}$.

Theorem (Blondel & Portier 2002)

The Bounded Skolem Problem is NP*-hard.*

Open question

Can we close the gap and show NP*-completeness?*

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Theorem (Bacik, O., Worrell 2026)

The Bounded Skolem Problem for Order k is in coRP.

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Theorem (Bacik, O., Worrell 2026)

The Bounded Skolem Problem for Order k is in coRP.

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1. using p-adic analysis, compute in polynomial time all of the polynomially many candidate indices $0 \leq n_1, n_2, \ldots, n_m \leq B$

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Theorem (Bacik, O., Worrell 2026)

The Bounded Skolem Problem for Order k is in coRP.

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

1. using p-adic analysis, compute in polynomial time all of the polynomially many candidate indices $0 \leq n_1, n_2, \ldots, n_m \leq B$
2. construct a polynomial-size arithmetic circuit C outputting the product $u_{n_1} u_{n_2} \cdots u_{n_m}$

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

Theorem (Bacik, O., Worrell 2026)

The Bounded Skolem Problem for Order k is in coRP.

1. using p-adic analysis, compute in polynomial time all of the polynomially many candidate indices $0 \leq n_1, n_2, \ldots, n_m \leq B$
2. construct a polynomial-size arithmetic circuit C outputting the product $u_{n_1} u_{n_2} \cdots u_{n_m}$
3. determine if $C = 0$ in coRP

The Bounded Skolem Problem: Complexity for fixed order

The Bounded Skolem Problem

Instance: LRS $\boldsymbol{u}$ and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

The Bounded Skolem Problem for Order k

Instance: LRS $\boldsymbol{u}$ of order k and bound B
Question: $\exists\, n \leq B$ s.t. $u_n = 0$?

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Theorem (Bacik, O., Worrell 2026)

The Bounded Skolem Problem for Order k is in coRP.

1. using p-adic analysis, compute in polynomial time all of the polynomially many candidate indices $0 \leq n_1, n_2, \ldots, n_m \leq B$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

Open questions

– Can we compute in polynomial time the candidate indices **without** *using p-adic analysis?*
– Can we derandomise this algorithm?

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$
- However, this LRS is **degenerate**: it can be decomposed as the interleaving of the two non-degenerate LRS $\langle 1, 2, 3, 4, \ldots \rangle$ and $\langle 0, 0, 0, 0, \ldots \rangle$

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$
- However, this LRS is **degenerate**: it can be decomposed as the interleaving of the two non-degenerate LRS $\langle 1, 2, 3, 4, \ldots \rangle$ and $\langle 0, 0, 0, 0, \ldots \rangle$
- This is a general phenomenon, and the decomposition is entirely mechanical

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$
- However, this LRS is **degenerate**: it can be decomposed as the interleaving of the two non-degenerate LRS $\langle 1, 2, 3, 4, \ldots \rangle$ and $\langle 0, 0, 0, 0, \ldots \rangle$
- This is a general phenomenon, and the decomposition is entirely mechanical

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS that is not identically zero. Then its set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ is finite.

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$
- However, this LRS is **degenerate**: it can be decomposed as the interleaving of the two non-degenerate LRS $\langle 1, 2, 3, 4, \ldots \rangle$ and $\langle 0, 0, 0, 0, \ldots \rangle$
- This is a general phenomenon, and the decomposition is entirely mechanical

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS that is not identically zero. Then its set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ is finite.

Unfortunately, all known proofs make use of non-constructive p-adic techniques

Zeros and non-degeneracy

Can LRS have arbitrarily large or even infinitely many zeros?

- Yes! For example, the sequence $\langle 1, 0, 2, 0, 3, 0, 4, 0, \ldots \rangle$, satisfying the recurrence $u_{n+4} = 2u_{n+2} - u_n$
- However, this LRS is **degenerate**: it can be decomposed as the interleaving of the two non-degenerate LRS $\langle 1, 2, 3, 4, \ldots \rangle$ and $\langle 0, 0, 0, 0, \ldots \rangle$
- This is a general phenomenon, and the decomposition is entirely mechanical

Theorem (Skolem 1934; Mahler 1935, 1956; Lech 1953)

Let $\langle u_0, u_1, u_2, \ldots \rangle$ be a non-degenerate LRS that is not identically zero. Then its set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ is finite.

Unfortunately, all known proofs make use of non-constructive p-adic techniques

- From now on, all our LRS are assumed to be non-degenerate and not identically zero

Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$$u_0 = 1$$
$$u_1 = 16$$
$$u_2 = 12$$
$$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

$\chi(x) = x^3 + 2x^2 - 3x - 10$

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

$\chi(x) = x^3 + 2x^2 - 3x - 10$

char. roots: $-2 + i$, $-2 - i$, 2

1	−392114	−1281554407154
16	6543432	2904329359752
12	−13596326	−4513760701286
34	42901808	4924965410288
128	−61158274	5652080673086
−34	115058712	−41666872128168
792	15425834	149539640378474
−406	−297258272	−367559090410592
2848	1791381166	767068380674926
1006	−4320278808	−1141417628796888
2472	11042118394	908449495512634
26554	−17131261552	2429531929333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594

Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

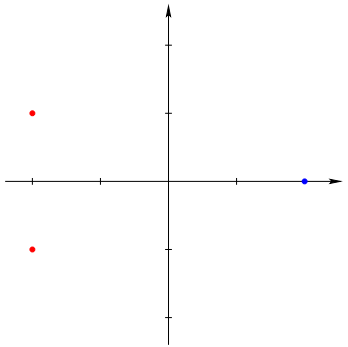
$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

$\chi(x) = x^3 + 2x^2 - 3x - 10$

char. roots: $-2 + i$, $-2 - i$, 2

1	−392114	−1281554407154
16	6543432	2904329359752
12		1286
34		0288
128		3086
−34		28168
792		378474
−406		410592
2848		674926
1006		8796888
2472		512634
26554		9333328
−35632	2418600206	−13547891660097634
175646	10655218872	43468874063321592
−192648	−120064782646	−103286103813602806
555914	513956123968	201499913216194048
66688	−1281554407154	−278169397239980594



Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

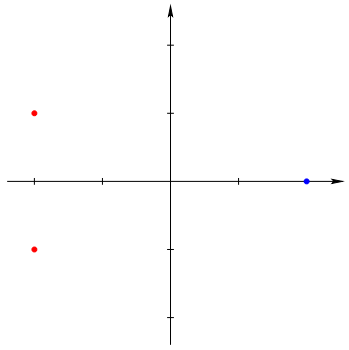
$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

$\chi(x) = x^3 + 2x^2 - 3x - 10$

char. roots: $-2 + i$, $-2 - i$, 2

1	−392114	−1281554407154
16	6543432	2904329359752
12		1286
34		0288
128		3086
−34		28168
792		378474
−406		410592
2848		674926
1006		8796888
2472		512634
26554		9333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592



$$u_n = \frac{-32 + 9i}{17}(-2 + i)^n + \frac{-32 - 9i}{17}(-2 - i)^n + \frac{81}{17}2^n$$

Back to our order-3 example

$$\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = \begin{pmatrix} 5 & -2 & 5 \\ 10 & 3 & -14 \\ 0 & 3 & -10 \end{pmatrix}^n \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

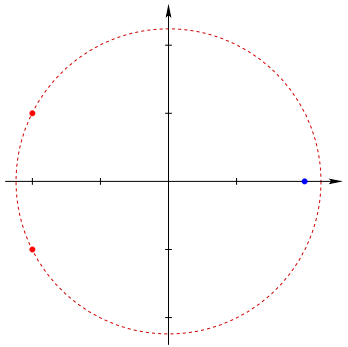
$u_0 = 1$
$u_1 = 16$
$u_2 = 12$

$u_{n+3} = -2u_{n+2} + 3u_{n+1} + 10u_n$

$\chi(x) = x^3 + 2x^2 - 3x - 10$

char. roots: $-2 + i$, $-2 - i$, 2

1	−392114	−1281554407154
16	6543432	2904329359752
12		1286
34		0288
128		3086
−34		28168
792		378474
−406		410592
2848		674926
1006		8796888
2472		512634
26554		9333328
−35632	24186090206	−13547891660097634
175646	10655218872	43468874063321592



$$u_n = \frac{-32 + 9i}{17}(-2 + i)^n + \frac{-32 - 9i}{17}(-2 - i)^n + \frac{81}{17}2^n$$

The Skolem Problem at orders up to 4

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Given a non-degenerate LRS $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ *with either*

(i) at most three dominant roots in modulus, or

(ii) at most two dominant roots with respect to some p-adic valuation,

there is a computable bound $B = 2^{\mathcal{O}(||\boldsymbol{u}||)}$ *such that, for* $n > B$, $u_n \neq 0$.

The Skolem Problem at orders up to 4

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Given a non-degenerate LRS $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ *with either*

(i) at most three dominant roots in modulus, or

(ii) at most two dominant roots with respect to some p-adic valuation,

there is a computable bound $B = 2^{\mathcal{O}(||\boldsymbol{u}||)}$ *such that, for* $n > B$, $u_n \neq 0$.

Corollary

For LRS of order 4 *or less, the Skolem Problem reduces to the Bounded Skolem Problem, and is therefore decidable in* coRP.

The Skolem Problem at orders up to 4

Theorem (Mignotte, Shorey, Tijdeman 1984; Vereshchagin 1985)

Given a non-degenerate LRS $\boldsymbol{u} = \langle u_0, u_1, u_2, \ldots \rangle$ *with either*

(i) at most three dominant roots in modulus, or

(ii) at most two dominant roots with respect to some p-adic valuation,

there is a computable bound $B = 2^{\mathcal{O}(||\boldsymbol{u}||)}$ *such that, for* $n > B$, $u_n \neq 0$.

Corollary

For LRS of order 4 *or less, the Skolem Problem reduces to the Bounded Skolem Problem, and is therefore decidable in* coRP.

One critical ingredient of the Mignotte *et al.* result is Baker's theorem on linear forms in logarithms of algebraic numbers, which earned Baker the Fields Medal in 1970

How large can zeros of arbitrary LRS get?

How large can zeros of arbitrary LRS get?

We do not know of a *single* instance of an LRS $\boldsymbol{u}$ with $u_n = 0$ for $n \geq 2^{2^{||\boldsymbol{u}||}}$!

How large can zeros of arbitrary LRS get?

We do not know of a *single* instance of an LRS $\boldsymbol{u}$ with $u_n = 0$ for $n \geq 2^{2^{||\boldsymbol{u}||}}$!

Of course, that doesn't mean such LRS don't exist

How large can zeros of arbitrary LRS get?

We do not know of a *single* instance of an LRS $\boldsymbol{u}$ with $u_n = 0$ for $n \geq 2^{2^{||\boldsymbol{u}||}}$!

Of course, that doesn't mean such LRS don't exist

But we now explain why there are very good reasons to expect the following:

How large can zeros of arbitrary LRS get?

We do not know of a *single* instance of an LRS $\boldsymbol{u}$ with $u_n = 0$ for $n \geq 2^{2^{||\boldsymbol{u}||}}$!

Of course, that doesn't mean such LRS don't exist

But we now explain why there are very good reasons to expect the following:

Conjecture

For any LRS $\boldsymbol{u}$, if $u_n = 0$, then $n < e^{e^{e^{||\boldsymbol{u}||}}}$.

A Brief History of Primes

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

How many primes are there from 0 up to x?

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

How many primes are there from 0 up to x?

$$\pi(x)$$

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

How many primes are there from 0 up to x?

$$\pi(x) \approx \int_0^x \frac{1}{\log t}\, dt$$

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

How many primes are there from 0 up to x?

$$\pi(x) \approx \int_0^x \frac{1}{\log t}\, dt \triangleq \mathrm{li}(x)$$

A Brief History of Primes

Theorem (Euclid c. 300 BC)

There are infinitely many prime numbers.

"As a boy [circa 1792], I considered the problem of how many primes there are up to a given point. From my calculations, I determined that the density of primes around x, is about $1/\log x$"

Gauss, in a letter to Encke

According to Gauss: the number of primes in blue segment is approximately $L \cdot \frac{1}{\log x}$

How many primes are there from 0 up to x?

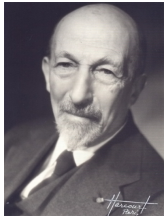
$$\pi(x) \approx \int_0^x \frac{1}{\log t}\, dt \triangleq \mathrm{li}(x) \sim \frac{x}{\log x}$$

A Brief History of Primes

Prime Number Theorem
(Hadamard & de la Vallée Poussin 1896)

$\pi(x) \sim \mathrm{li}(x)$ $\left(\sim \frac{x}{\log x} \right)$.

In other words, $\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$

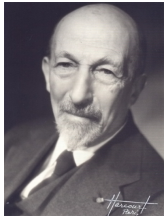


A Brief History of Primes

Prime Number Theorem
(Hadamard & de la Vallée Poussin 1896)

$\pi(x) \sim \mathrm{li}(x)$ $\left(\sim \frac{x}{\log x} \right)$.

In other words, $\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$



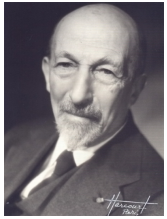
But the Prime Number Theorem says *nothing* about the difference $|\pi(x) - \mathrm{li}(x)|$!

A Brief History of Primes

Prime Number Theorem
(Hadamard & de la Vallée Poussin 1896)

$\pi(x) \sim \mathrm{li}(x)$ $\left(\sim \frac{x}{\log x} \right)$.

In other words, $\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$



But the Prime Number Theorem says *nothing* about the difference $|\pi(x) - \mathrm{li}(x)|$!

This is where the Riemann Hypothesis comes in ...

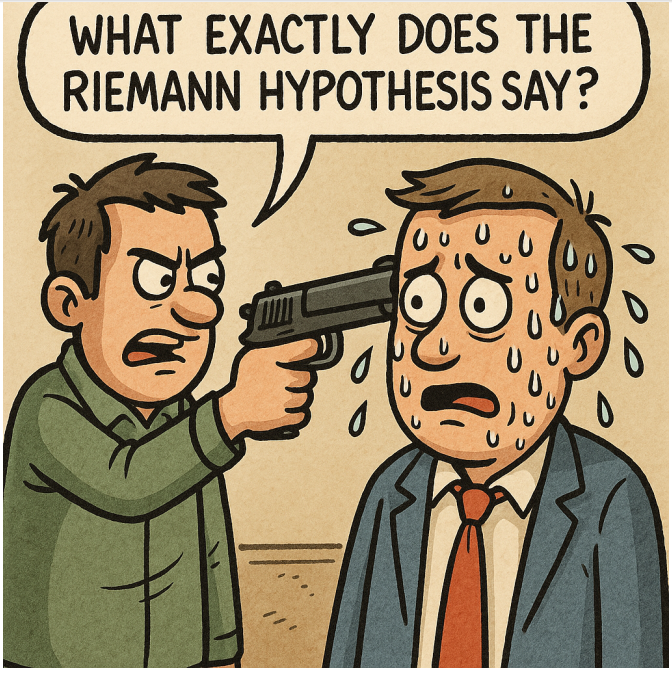
Theorem (von Koch 1901)

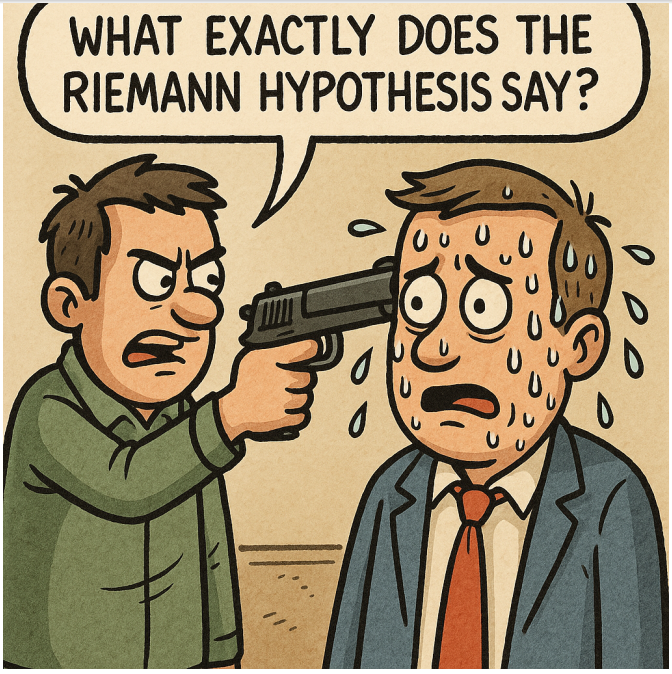
Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

Theorem (von Koch 1901)

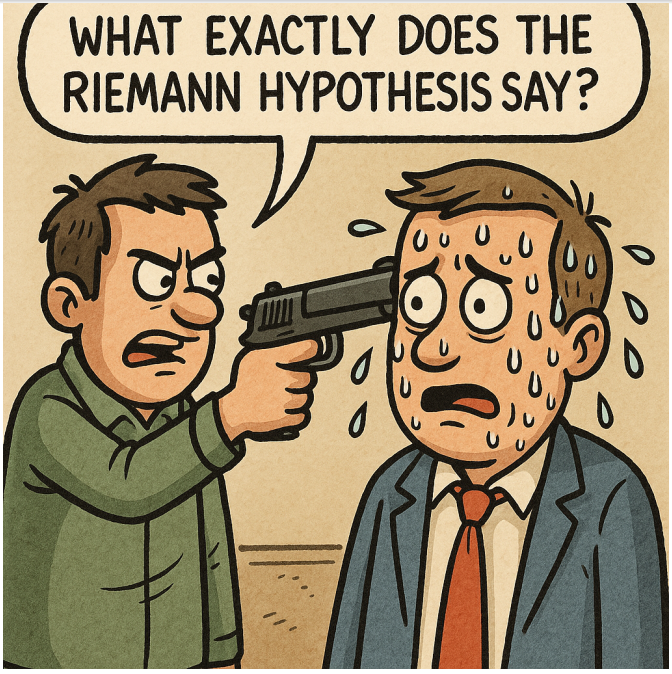
Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

In fact, this assertion is equivalent to the Riemann Hypothesis!


WHAT EXACTLY DOES THE RIEMANN HYPOTHESIS SAY?

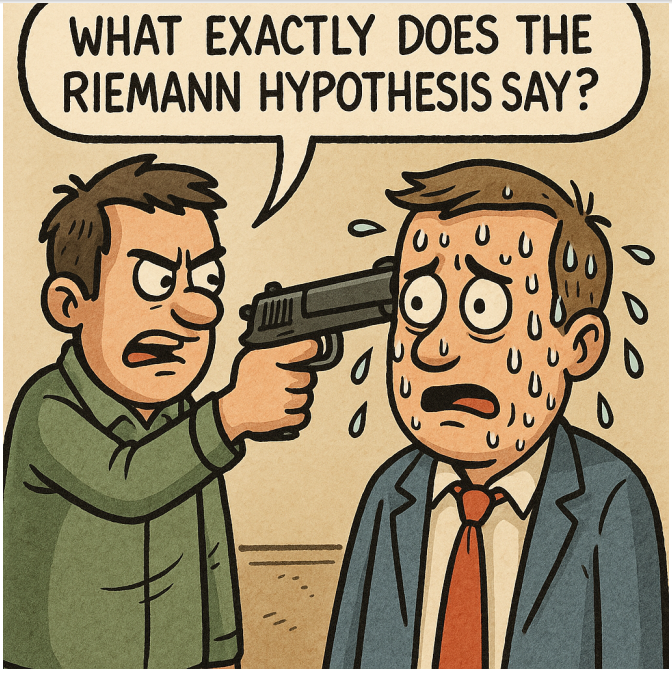


$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$



$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

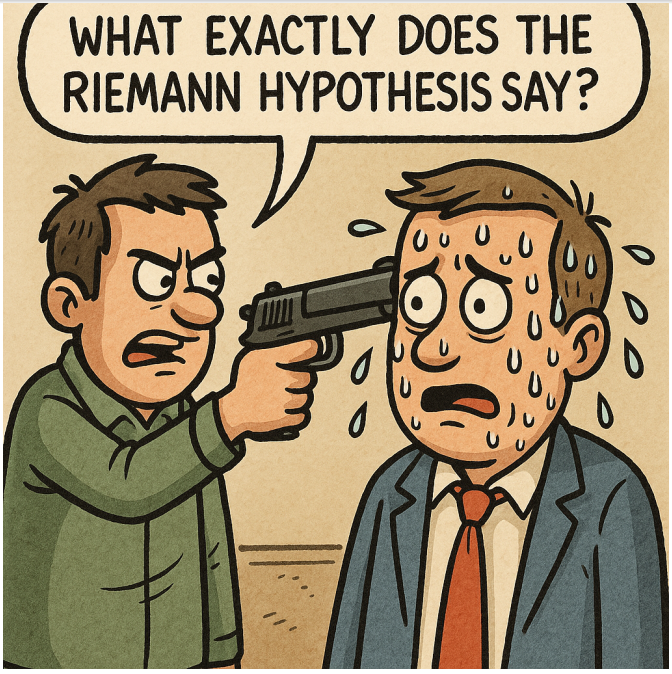
$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$



$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

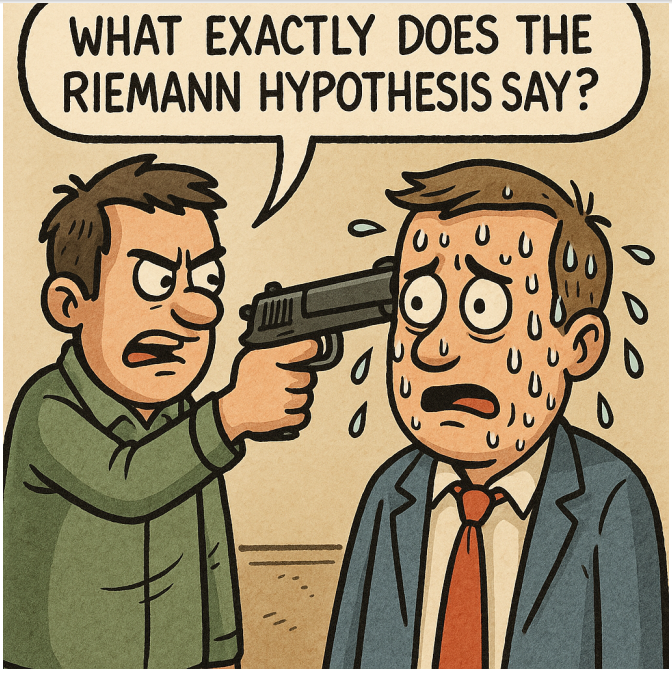


$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Need to extend $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$



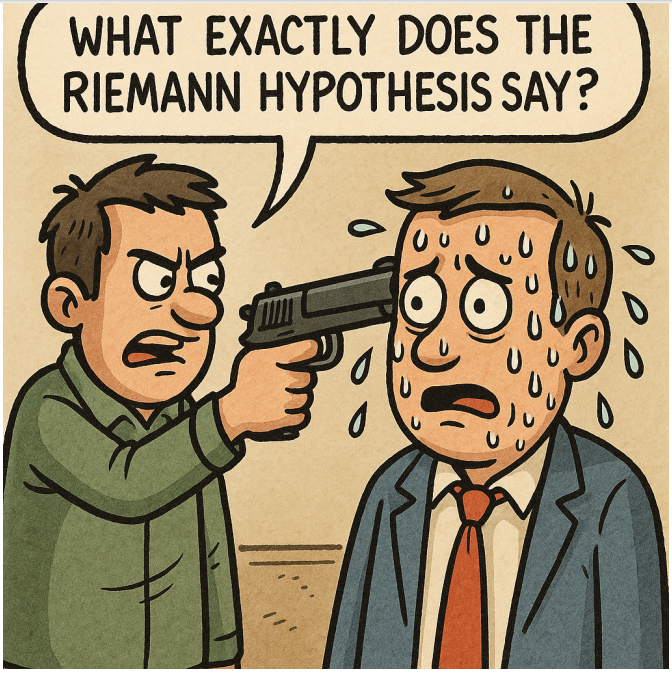
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Need to extend $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$

$$\zeta(-1) =$$



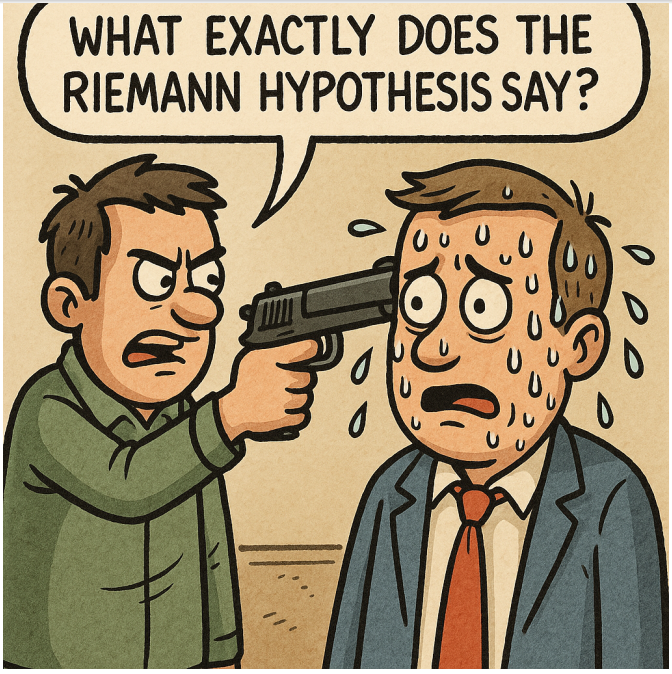
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Need to extend $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$

$$\zeta(-1) = \frac{1}{1^{-1}} + \frac{1}{2^{-1}} + \frac{1}{3^{-1}} + \cdots$$



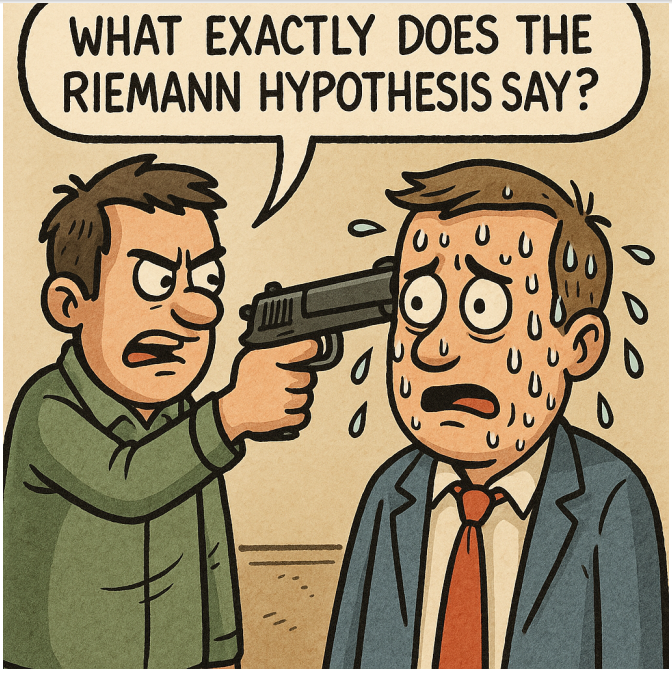
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Need to extend $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$

$$\zeta(-1) = \frac{1}{1^{-1}} + \frac{1}{2^{-1}} + \frac{1}{3^{-1}} + \cdots$$
$$= 1 + 2 + 3 + \cdots =$$



$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(1) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Need to extend $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$

$$\begin{aligned} \zeta(-1) &= \frac{1}{1^{-1}} + \frac{1}{2^{-1}} + \frac{1}{3^{-1}} + \cdots \\ &= 1 + 2 + 3 + \cdots = -\frac{1}{12} \end{aligned}$$

Theorem (von Koch 1901)

Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

In fact, this assertion is equivalent to the Riemann Hypothesis!

Theorem (von Koch 1901)

Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

In fact, this assertion is equivalent to the Riemann Hypothesis!

Schoenfeld showed that, assuming R.H., for $x \geq 2657$, $|\pi(x) - \mathrm{li}(x)| < \dfrac{\sqrt{x}\log x}{8\pi}$.

Theorem (von Koch 1901)

Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

In fact, this assertion is equivalent to the Riemann Hypothesis!

Schoenfeld showed that, assuming R.H., for $x \geq 2657$, $|\pi(x) - \mathrm{li}(x)| < \dfrac{\sqrt{x}\log x}{8\pi}$.

There are many unconditional estimates for the error term, e.g.:

Theorem (von Koch 1901)

Assuming the Riemann Hypothesis, $|\pi(x) - \mathrm{li}(x)| = O(\sqrt{x}\log x)$.

In fact, this assertion is equivalent to the Riemann Hypothesis!

Schoenfeld showed that, assuming R.H., for $x \geq 2657$, $|\pi(x) - \mathrm{li}(x)| < \dfrac{\sqrt{x}\log x}{8\pi}$.

There are many unconditional estimates for the error term, e.g.:

Theorem (Trudgian 2016)

For $x \geq 229$, $|\pi(x) - \mathrm{li}(x)| \leq 0.2795 \dfrac{x}{(\log x)^{3/4}} \exp\left(-\sqrt{\dfrac{\log x}{6.455}}\right)$.

Mind the Gap!

Mind the Gap!

Mind the Gap!

- Define $G(x) := \max\{p_{n+1} - p_n : p_n \leq x\}$

Mind the Gap!

- Define $G(x) := \max\{p_{n+1} - p_n : p_n \leq x\}$

Theorem (Baker, Harman, Pintz 2001)

$G(x) = O(x^{0.525})$.

Mind the Gap!

- Define $G(x) := \max\{p_{n+1} - p_n : p_n \leq x\}$

Theorem (Baker, Harman, Pintz 2001)

$G(x) = O(x^{0.525})$.

Theorem (Cramér 1919)

Assuming the Riemann Hypothesis, $G(x) = O(\sqrt{x}\log x)$.

Mind the Gap!

- Define $G(x) := \max\{p_{n+1} - p_n : p_n \leq x\}$

Theorem (Baker, Harman, Pintz 2001)

$G(x) = O(x^{0.525})$.

Theorem (Cramér 1919)

Assuming the Riemann Hypothesis, $G(x) = O(\sqrt{x}\log x)$.

On the other hand:

Theorem (Ford, Green, Konyagin, Maynard, Tao 2017)

$$G(x) = \Omega\left(\log x \frac{(\log\log x)(\log\log\log\log x)}{\log\log\log x}\right).$$

The Cramér Random Model

"In investigations concerning the asymptotic properties of arithmetic functions, it is often possible to make an interesting heuristic use of probability arguments"

Cramér, 1937

The Cramér Random Model

"In investigations concerning the asymptotic properties of arithmetic functions, it is often possible to make an interesting heuristic use of probability arguments"

Cramér, 1937

Now **if** the sequence of prime numbers **were** a truly random set of integers with density $1/\log x$, then with probability 1:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1$$

The Cramér Random Model

"In investigations concerning the asymptotic properties of arithmetic functions, it is often possible to make an interesting heuristic use of probability arguments"

Cramér, 1937

Now **if** the sequence of prime numbers **were** a truly random set of integers with density $1/\log x$, then with probability 1:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1$$

Conjecture (Cramér, 1935; Granville, 2011)

There exists $\kappa \geq 1$ *such that, for all* x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

The Cramér Random Model

"In investigations concerning the asymptotic properties of arithmetic functions, it is often possible to make an interesting heuristic use of probability arguments"

Cramér, 1937

Now **if** the sequence of prime numbers **were** a truly random set of integers with density $1/\log x$, then with probability 1:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1$$

Conjecture (Cramér, 1935; Granville, 2011)

There exists $\kappa \geq 1$ such that, for all x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Granville argues that in fact $\kappa = 2e^{-\gamma} \approx 1.1229$

The Cramér Random Model

"In investigations concerning the asymptotic properties of arithmetic functions, it is often possible to make an interesting heuristic use of probability arguments"

Cramér, 1937

Now **if** the sequence of prime numbers **were** a truly random set of integers with density $1/\log x$, then with probability 1:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1$$

Conjecture (Cramér, 1935; Granville, 2011)

There exists $\kappa \geq 1$ such that, for all x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Granville argues that in fact $\kappa = 2e^{-\gamma} \approx 1.1229$

The largest observed value for κ is approx. 0.9206 for $p_n = 1693182318746371$

Cramér vs. Cramér

Cramér-Granville Conjecture

There exists $\kappa \geq 1$ *such that, for all* x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Cramér vs. Cramér

Cramér-Granville Conjecture

There exists $\kappa \geq 1$ *such that, for all* x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Strengthened Cramér Conjecture

There exists $\eta \geq 1$ *such that, for all* x, $\max\{g_{n+1} - g_n : g_n \leq x\} \leq \eta \log^2 x$.

Cramér vs. Cramér

Cramér-Granville Conjecture

There exists $\kappa \geq 1$ *such that, for all* x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Strengthened Cramér Conjecture

There exists $\eta \geq 1$ *such that, for all* x, $\max\{g_{n+1} - g_n : g_n \leq x\} \leq \eta \log^2 x$.

Theorem (Luca, O., Worrell 2025, 2026)

Let $\boldsymbol{u}$ *be a non-degenerate integer LRS that is not identically zero.*
Assuming the Strengthened Cramér Conjecture, for all $n \geq e^{e^{e^{(||\boldsymbol{u}||)}}}$, $u_n \neq 0$.

Cramér vs. Cramér

Cramér-Granville Conjecture

There exists $\kappa \geq 1$ *such that, for all* x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Strengthened Cramér Conjecture

There exists $\eta \geq 1$ *such that, for all* x, $\max\{g_{n+1} - g_n : g_n \leq x\} \leq \eta \log^2 x$.

Theorem (Luca, O., Worrell 2025, 2026)

Let $\boldsymbol{u}$ *be a non-degenerate integer LRS that is not identically zero.*
Assuming the Strengthened Cramér Conjecture, for all $n \geq e^{e^{e^{(||\boldsymbol{u}||)}}}$, $u_n \neq 0$.

Corollary

The Skolem Problem is decidable subject to the Strengthened Cramér Conjecture.

Cramér vs. Cramér

Cramér-Granville Conjecture

There exists $\kappa \geq 1$ such that, for all x, $\max\{p_{n+1} - p_n : p_n \leq x\} \leq \kappa \log^2 x$.

Strengthened Cramér Conjecture

There exists $\eta \geq 1$ such that, for all x, $\max\{g_{n+1} - g_n : g_n \leq x\} \leq \eta \log^2 x$.

Theorem (Luca, O., Worrell 2025, 2026)

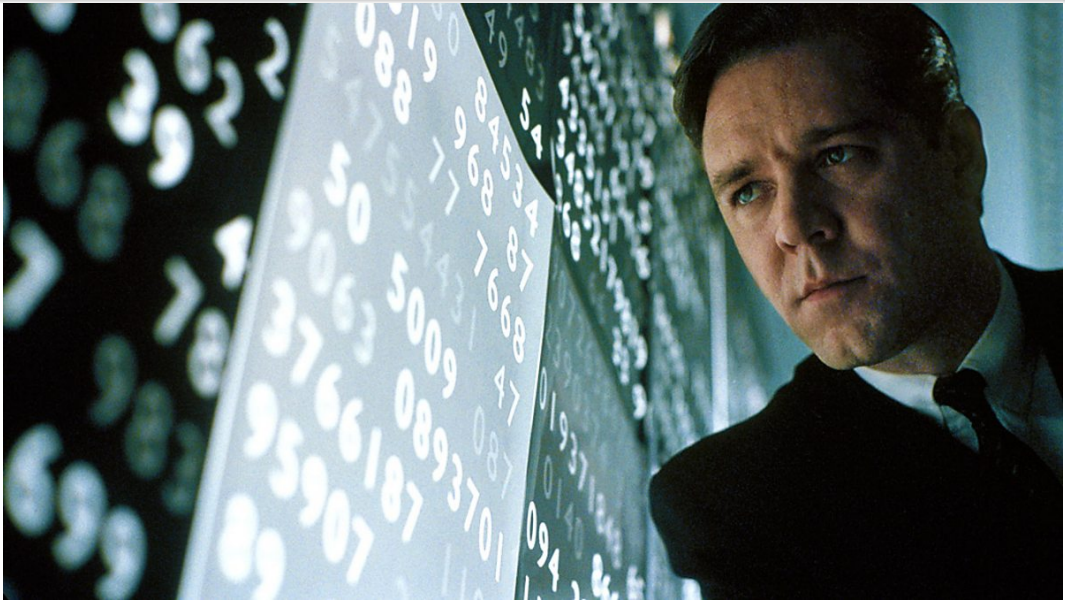
Let $\boldsymbol{u}$ be a non-degenerate integer LRS that is not identically zero.
Assuming the Strengthened Cramér Conjecture, for all $n \geq e^{e^{e^{(||\boldsymbol{u}||)}}}$, $u_n \neq 0$.

Corollary

The Skolem Problem is decidable subject to the Strengthened Cramér Conjecture.

Note however that this is a completely impractical ("galactic") algorithm!!

Could AI spot patterns/proofs that have so far escaped us?



A hard sequence to crack

12, 49, 374, 6003, 21520, 150773, 2711418, 7228087, 39896084, 1077651897, 8443088
62, −5193511429, 348581351448, −1315000789379, −17484999866494, 65954891227
455, −1593947490748388, −16419811303845055, −19999927574998650, −12346719
08617403261, −11641249143376659424, −31686908910032347131, −7877424714701
85791606, −707552669458875569157 7, −223216436161220108317660, −44017099056
0193300087607, −38277865764737241740693 62, −11455105026466370320565493, −
21856523787155407261973909 6, −18563382775690197179626184 83, −41978320729 7
0077529712375918, −95126084985010283959648793009, −79447079006271641313 99
29419732, −50535760574704274425851005 1759, −34183642949757679223770805575
274, −28367553015751143340489657218 2125, 89281617766593850971014560526443
2, −79304779679502066573776559438 59435, −68314840318113280928556102740451
430, 11321357606927679970712702221712191 59, 12977188722056728730655277098 0
1657396, 61000319054305640349531041718423264 89, 92354561340330113693370382
7562576691614, 32677050680355530737676821325803899228 43, 21983703673232747
72574780900096397342316 0, 62380530341906333381629623294905705791401 3, 2743
70143875558146989317028308044475442985 8, 18327472900837342172233173469094
562675800927, 37262999008769214888126859529103249430014 5724, 1735532316107

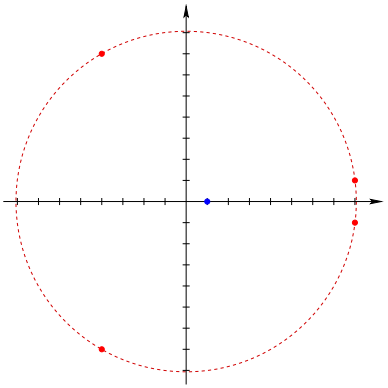
A hard sequence to crack

$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$

1077651897, 8443088
866494, 65954891227
455, −1593947490748388, −16419811303845055, −19999927574998650, −12346719
08617403261, −11641249143376659424, −31686908910032347131, −7877424714701
85791606, −70755266945887555691577, −22321643616220108317660, −44017099056
0193300087607, −38277865764737241740693362, −11455105026466370320565493, −
21856523787155407261973909 6, −18563382775690197179626184 83, −419783207297
0077529712375918, −95126084985010283959648793009, −79447079006271641313 99
29419732, −50535760574704274425851005 1759, −34183642949757679223770805575
274, −28367553015751143340489657218 2125, 89281617766593850971014560526443
2, −79304779679502066573776559438 59435, −68314840318113280928556102740451
430, 11321357606927679970712702221712 19159, 12977188722056728730655277098 0
1657396, 61000319054305640349531041718423 26489, 92354561340330113693370382
7562576691614, 32677050680355530737676821325803899 22843, 21983703673232747
72574780900096397342316 0, 62380530341906333381629623294905705791 4013, 2743
70143875558146989317028308044475442 9858, 18327472900837342172233173469094
562675800927, 37262999008769214888126859529103249430014 5724, 1735532316107

A hard sequence to crack

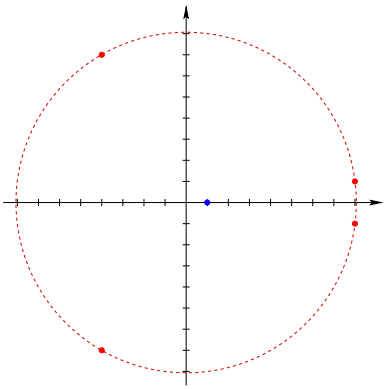
$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$



A hard sequence to crack

$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$

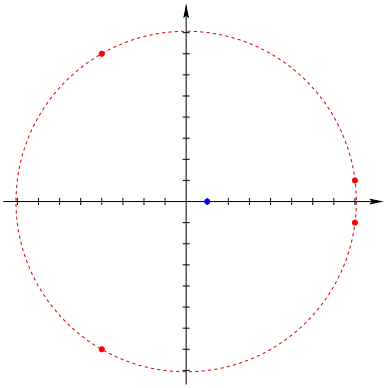
- $\boldsymbol{u}$ has infinitely many positive and negative terms



A hard sequence to crack

$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$

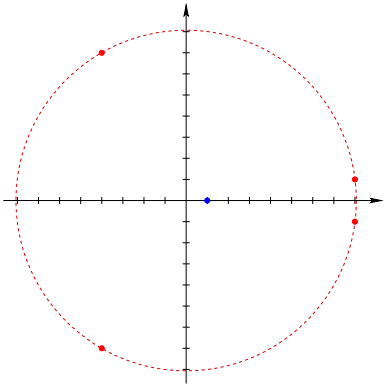
- $\boldsymbol{u}$ has infinitely many positive and negative terms
- $\boldsymbol{u}$ has no zeros in $[0, 10^{1000}]$



A hard sequence to crack

$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$

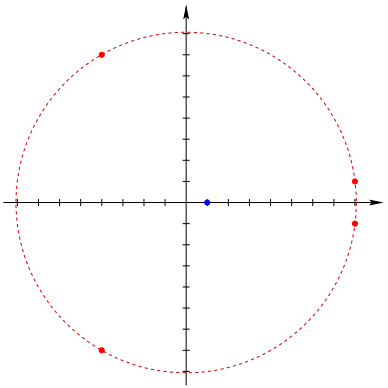
- $\boldsymbol{u}$ has infinitely many positive and negative terms
- $\boldsymbol{u}$ has no zeros in $[0, 10^{1000}]$
- $\boldsymbol{u}$ has at most *one* zero



A hard sequence to crack

$$u_n = 2(-4+7i)^n + 2(-4-7i)^n + 4(8+i)^n + 4(8-i)^n + n$$

- $\boldsymbol{u}$ has infinitely many positive and negative terms
- $\boldsymbol{u}$ has no zeros in $[0, 10^{1000}]$
- $\boldsymbol{u}$ has at most *one* zero



Open question

How can one prove that $\boldsymbol{u}$ has no zeros?

Outlook