Mahler measure

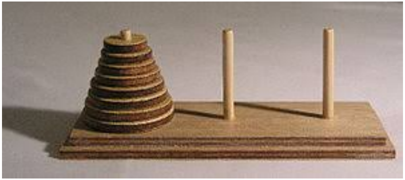
A journey from Mersenne primes to special values of L-functions

Subham Roy

Univerzita Karlova

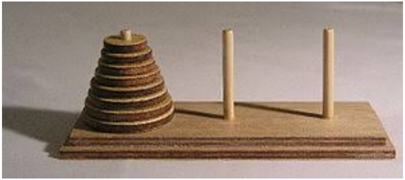
Algebra Colloquium
October 22, 2024

Tower of Hanoi



The objective is to move the entire stack to one of the other rods, obeying three rules.

Tower of Hanoi

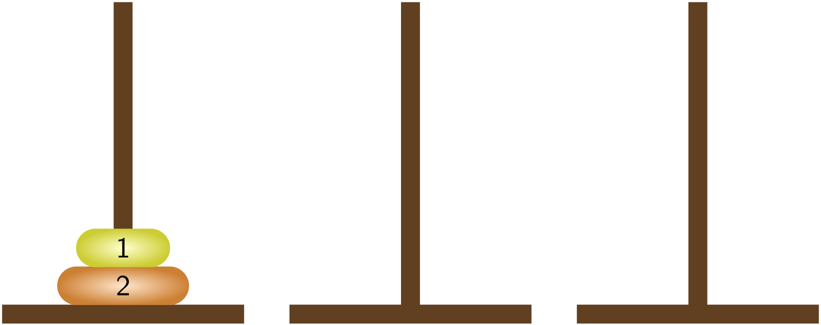


The objective is to move the entire stack to one of the other rods, obeying three rules.

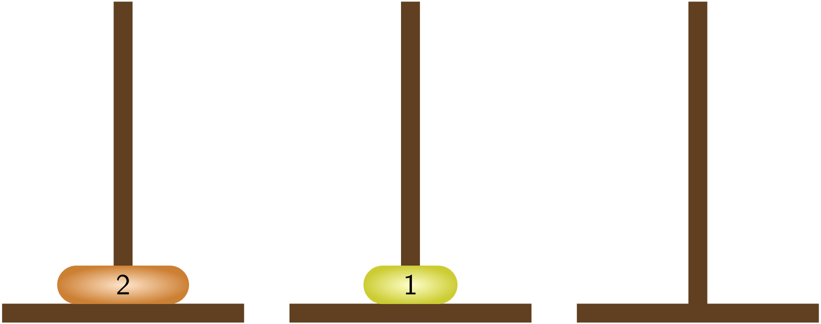
Rules

1. Only one disk may be moved at a time.
2. Each move consists of taking the upper disk from one of the stacks and placing it on top of another stack or on an empty rod.
3. No disk may be placed on top of a disk that is smaller than it.

Tower of Hanoi – 2 Discs

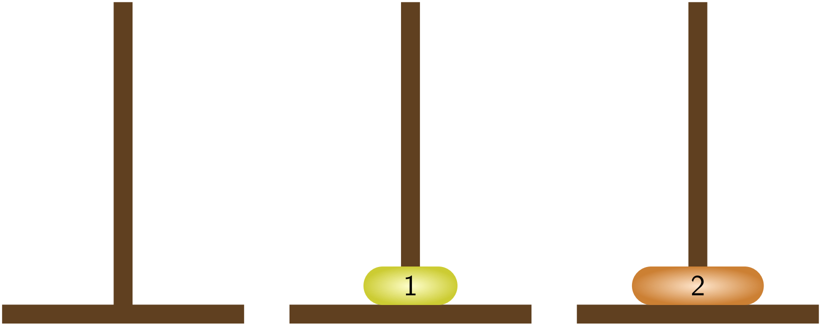


Tower of Hanoi – 2 Discs



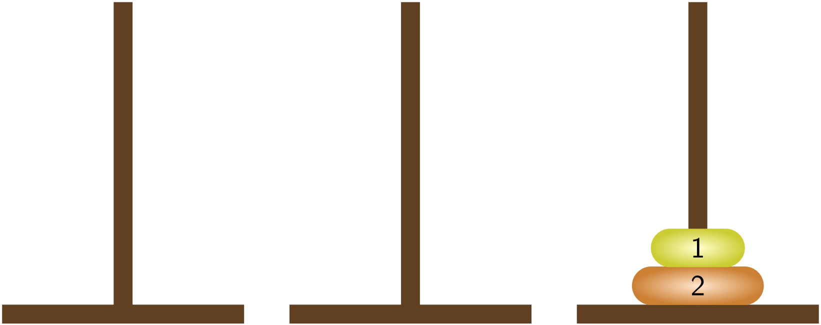
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 2 Discs



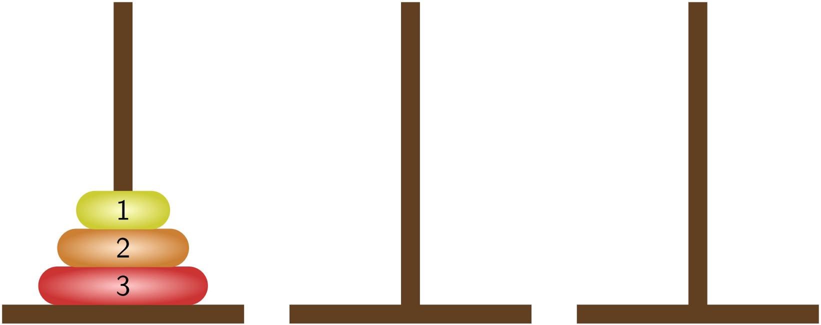
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 2 Discs

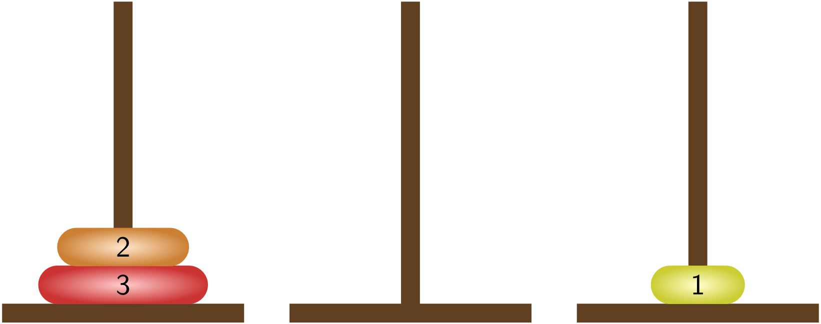


Moved disc from pole 2 to pole 3.

Tower of Hanoi – 3 Discs

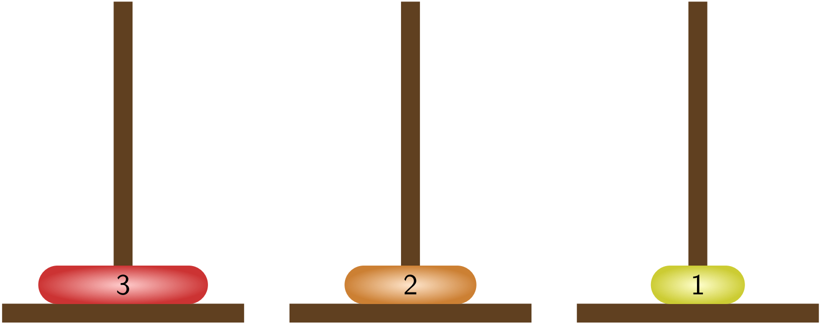


Tower of Hanoi – 3 Discs



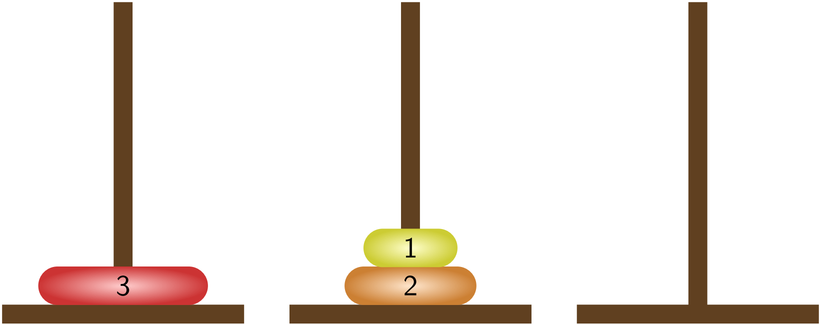
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 3 Discs



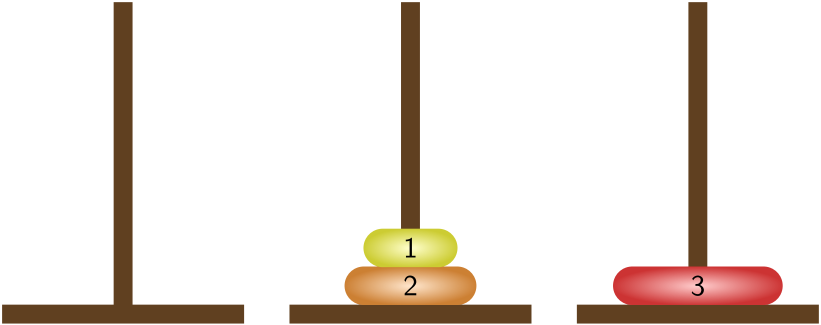
Moved disc from pole 1 to pole 2.

Tower of Hanoi – 3 Discs



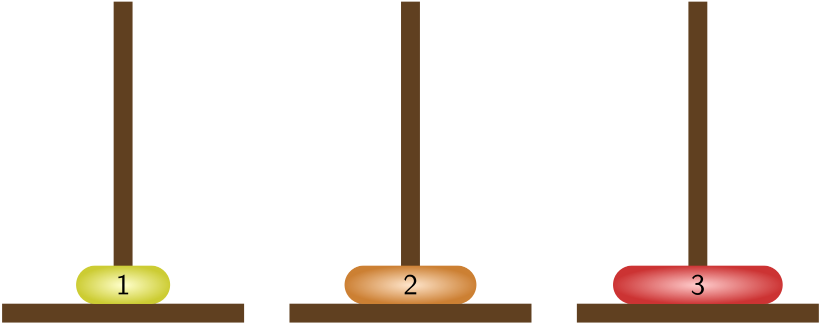
Moved disc from pole 3 to pole 2.

Tower of Hanoi – 3 Discs



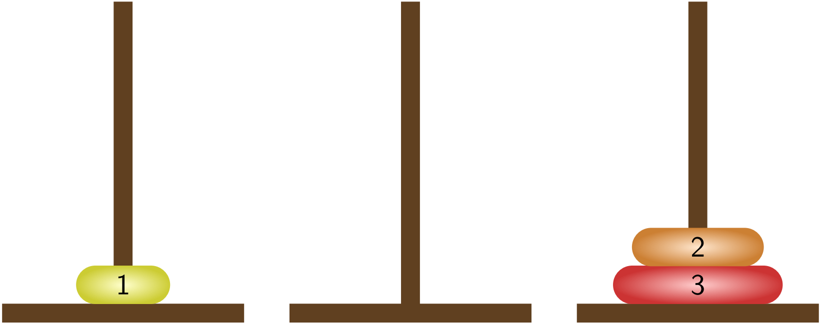
Moved disc from pole 1 to pole 3.

Tower of Hanoi – 3 Discs



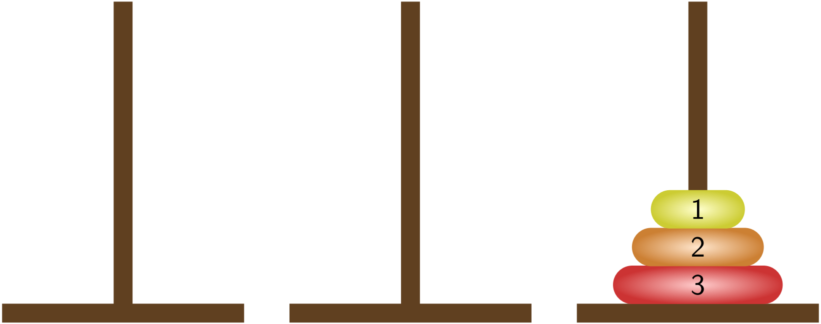
Moved disc from pole 2 to pole 1.

Tower of Hanoi – 3 Discs



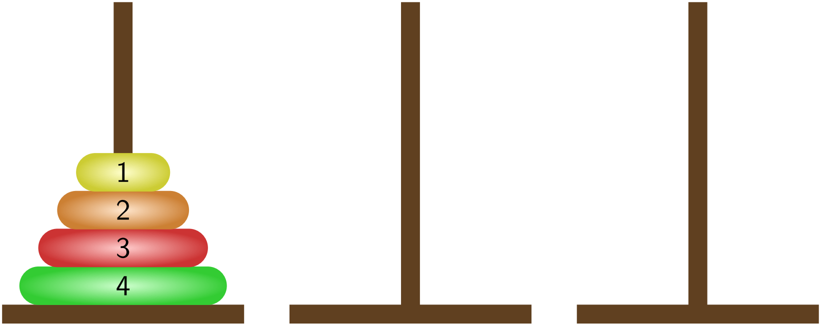
Moved disc from pole 2 to pole 3.

Tower of Hanoi – 3 Discs



Moved disc from pole 1 to pole 3.

Tower of Hanoi – 4 Disc



Minimum number of moves?

Minimum number of moves

n=1 Minimum number of moves $1 = 2^1 - 1$.

n=2 Minimum number of moves $3 = 2^2 - 1$.

n=3 Minimum number of moves $7 = 2^3 - 1$.

Minimum number of moves

n=1 Minimum number of moves $1 = 2^1 - 1$.

n=2 Minimum number of moves $3 = 2^2 - 1$.

n=3 Minimum number of moves $7 = 2^3 - 1$.

n=4 Minimum number of moves $15 = 2^4 - 1$.

Minimum number of moves

n=1 Minimum number of moves $1 = 2^1 - 1$.

n=2 Minimum number of moves $3 = 2^2 - 1$.

n=3 Minimum number of moves $7 = 2^3 - 1$.

n=4 Minimum number of moves $15 = 2^4 - 1$.

$\vdots$

n Minimum number of moves $2^n - 1$.

Minimum number of moves

n=1 Minimum number of moves $1 = 2^1 - 1$.

n=2 Minimum number of moves $3 = 2^2 - 1$.

n=3 Minimum number of moves $7 = 2^3 - 1$.

n=4 Minimum number of moves $15 = 2^4 - 1$.

$\vdots$

n Minimum number of moves $2^n - 1$.

Definition (Marin Mersenne, early 17th Century)

A *Mersenne Number* is a number of the form $M_n = 2^n - 1$, where n is a positive integer.

Mersenne Primes

Note that if $n = ab$ (for $a, b \geq 1$),

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1\right).$$

For example, $2^3 - 1 = 7$ is a prime, but $2^4 - 1 = 15 = 3 \times 5$ is not.

Mersenne Primes

Note that if $n = ab$ (for $a, b \geq 1$),

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1\right).$$

For example, $2^3 - 1 = 7$ is a prime, but $2^4 - 1 = 15 = 3 \times 5$ is not.

Definition

A *Mersenne prime* is a prime of the form $M_p = 2^p - 1$, where p is a prime number.

Mersenne Primes

Note that if $n = ab$ (for $a, b \geq 1$),

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1\right).$$

For example, $2^3 - 1 = 7$ is a prime, but $2^4 - 1 = 15 = 3 \times 5$ is not.

Definition

A *Mersenne prime* is a prime of the form $M_p = 2^p - 1$, where p is a prime number.

M_n increases exponentially with n. In particular,

$$\frac{M_{n+1}}{M_n} \to 2, \text{ as } n \to \infty.$$

We expect the set $\{M_p : p \text{ is a prime}\}$ to contain *very large primes*.

A *perfect* appearance

Definition

A *perfect number* is a positive integer that is equal to the sum of its positive proper divisors. In other words, n is perfect number if $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} d$.

A *perfect* appearance

Definition

A *perfect number* is a positive integer that is equal to the sum of its positive proper divisors. In other words, n is perfect number if $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} d$.

Euclid's Elements (300 BCE):

If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect.

A *perfect* appearance

Definition

A *perfect number* is a positive integer that is equal to the sum of its positive proper divisors. In other words, n is perfect number if $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} d$.

Euclid's Elements (300 BCE):

If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect.

In a simpler term, if $2^p - 1 = M_p$ is a prime then $2^{p-1}M_p$ is a perfect number.

A *perfect* appearance

Definition

A *perfect number* is a positive integer that is equal to the sum of its positive proper divisors. In other words, n is perfect number if $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} d$.

Euclid's Elements (300 BCE):

If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect.

In a simpler term, if $2^p - 1 = M_p$ is a prime then $2^{p-1}M_p$ is a perfect number.

In the 18th century, Euler showed that all even perfect numbers are of the form $2^{p-1}M_p$, when M_p is a prime.

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.
- Frank N. Cole (1903): M_{67} is NOT a prime:

$$M_{67} = 147{,}573{,}952{,}589{,}676{,}412{,}927 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.

- Frank N. Cole (1903): M_{67} is NOT a prime:

$$M_{67} = 147{,}573{,}952{,}589{,}676{,}412{,}927 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

- If a prime q divides M_p, then $8 \mid (q \pm 1)$ and $q = 2kp + 1$, for some $k \in \mathbb{N}$.

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.

- Frank N. Cole (1903): M_{67} is NOT a prime:

$$M_{67} = 147{,}573{,}952{,}589{,}676{,}412{,}927 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

- If a prime q divides M_p, then $8 \mid (q \pm 1)$ and $q = 2kp + 1$, for some $k \in \mathbb{N}$.

193,707,721 is a prime and $193{,}707{,}721 - 1 = 8 \times 24{,}213{,}465.$

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.

- Frank N. Cole (1903): M_{67} is NOT a prime:

$$M_{67} = 147{,}573{,}952{,}589{,}676{,}412{,}927 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

- If a prime q divides M_p, then $8 \mid (q \pm 1)$ and $q = 2kp + 1$, for some $k \in \mathbb{N}$.

$$193{,}707{,}721 \text{ is a prime} \quad \text{and} \quad 193{,}707{,}721 - 1 = 8 \times 24{,}213{,}465.$$

- For primes p such that $4 \mid p - 3$, $2p + 1$ is a prime if and only if $2p + 1 \mid M_p$.

Finding Mersenne Primes

- Mersenne's list contains $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}$ and others, which he claimed are prime numbers.

- Frank N. Cole (1903): M_{67} is NOT a prime:

$$M_{67} = 147{,}573{,}952{,}589{,}676{,}412{,}927 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

- If a prime q divides M_p, then $8 \mid (q \pm 1)$ and $q = 2kp + 1$, for some $k \in \mathbb{N}$.

$$193{,}707{,}721 \text{ is a prime} \quad \text{and} \quad 193{,}707{,}721 - 1 = 8 \times 24{,}213{,}465.$$

- For primes p such that $4 \mid p - 3$, $2p + 1$ is a prime if and only if $2p + 1 \mid M_p$.

$$\text{For } p = 23, 4 \mid (p - 3) \quad \text{and} \quad 2p + 1 = 47 \mid 761{,}838{,}257{,}287.$$

Primality test

Lucas-Lehmer test (E. Lucas 1878, D. H. Lehmer 1930)

Consider the sequence S_n for $n \geq 1$:

$$S_1 = 4, S_n = S_{n-1}^2 - 2.$$

Then M_p is a prime if and only if $M_p \mid S_{p-1}$.

Primality test

Lucas-Lehmer test (E. Lucas 1878, D. H. Lehmer 1930)

Consider the sequence S_n for $n \geq 1$:

$$S_1 = 4, S_n = S_{n-1}^2 - 2.$$

Then M_p is a prime if and only if $M_p \mid S_{p-1}$.

Known *Mersenne primes* M_p (till now the number is ~~51~~ 52):

$$\{p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161, 74207281, 77232917, 82589933, 136279841\}$$

Primality test

Lucas-Lehmer test (E. Lucas 1878, D. H. Lehmer 1930)

Consider the sequence S_n for $n \geq 1$:

$$S_1 = 4, S_n = S_{n-1}^2 - 2.$$

Then M_p is a prime if and only if $M_p \mid S_{p-1}$.

Known *Mersenne primes* M_p (till now the number is ~~51~~ 52):

$$\{p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161, 74207281, 77232917, 82589933, 136279841\}$$

Largest known prime number: Mersenne prime of ~~24,862,048~~ 41,024,320 digits (*Great Internet Mersenne Prime Search (GIMPS), Luke Durant*, ~~2018~~ yesterday!!)

Why do we care about large primes?

- Following in the footsteps of Fermat, Mersenne, Leibniz, Euler, Lucas, Catalan, Putnam, Lehmer, and others. (a.k.a *Traditional values*!)

Why do we care about large primes?

- Following in the footsteps of Fermat, Mersenne, Leibniz, Euler, Lucas, Catalan, Putnam, Lehmer, and others. (a.k.a *Traditional values*!)
- Mersenne primes are among the simplest types of primes and have a range of applications. Their primality test is simple and elegant. (a.k.a. *Collectibles*!)

Why do we care about large primes?

- Following in the footsteps of Fermat, Mersenne, Leibniz, Euler, Lucas, Catalan, Putnam, Lehmer, and others. (a.k.a *Traditional values*!)
- Mersenne primes are among the simplest types of primes and have a range of applications. Their primality test is simple and elegant. (a.k.a. *Collectibles*!)
- "GIMPS project were used by Intel to test Pentium II and Pentium Pro chips before they were shipped." (a.k.a. *Hardware testing 101*!)

Why do we care about large primes?

- Following in the footsteps of Fermat, Mersenne, Leibniz, Euler, Lucas, Catalan, Putnam, Lehmer, and others. (a.k.a *Traditional values*!)
- Mersenne primes are among the simplest types of primes and have a range of applications. Their primality test is simple and elegant. (a.k.a. *Collectibles*!)
- "GIMPS project were used by Intel to test Pentium II and Pentium Pro chips before they were shipped." (a.k.a. *Hardware testing 101*!)
- Pizes for the first hundred-million digit prime (150000 USD), and the first billion digit prime (250000 USD). (a.k.a *For the money*!)

Why do we care about large primes?

- Following in the footsteps of Fermat, Mersenne, Leibniz, Euler, Lucas, Catalan, Putnam, Lehmer, and others. (a.k.a *Traditional values*!)
- Mersenne primes are among the simplest types of primes and have a range of applications. Their primality test is simple and elegant. (a.k.a. *Collectibles*!)
- "GIMPS project were used by Intel to test Pentium II and Pentium Pro chips before they were shipped." (a.k.a. *Hardware testing 101*!)
- Pizes for the first hundred-million digit prime (150000 USD), and the first billion digit prime (250000 USD). (a.k.a *For the money*!)
- *To understand the distribution of primes.*

What about non-Mersenne primes?

- 5 is not a Mersenne prime, neither is 193,707,721 (one of the prime divisor of M_{67}).

What about non-Mersenne primes?

- 5 is not a Mersenne prime, neither is 193,707,721 (one of the prime divisor of M_{67}).
- Can we form a primality test by divisibility for non-Mersenne primes?

What about non-Mersenne primes?

- 5 is not a Mersenne prime, neither is 193,707,721 (one of the prime divisor of M_{67}).
- Can we form a primality test by divisibility for non-Mersenne primes?
- Note that $\mathrm{Res}(X-2, X^n-1) = 2^n - 1 = M_n$, where, for polynomials $P, Q \in \mathbb{C}[X]$, the *resultant* $\mathrm{Res}(P,Q)$ is defined as

$$\mathrm{Res}(P,Q) = \prod_{\alpha_i} Q(\alpha_i) = \prod_{\beta_j} P(\beta_j),$$

with $P(X) = \prod_{i=1}^{r}(X-\alpha_i)$ and $Q(X) = \prod_{j=1}^{s}(X-\beta_j)$.

What about non-Mersenne primes?

- 5 is not a Mersenne prime, neither is 193,707,721 (one of the prime divisor of M_{67}).
- Can we form a primality test by divisibility for non-Mersenne primes?
- Note that $\mathrm{Res}(X-2, X^n-1) = 2^n - 1 = M_n$, where, for polynomials $P, Q \in \mathbb{C}[X]$, the *resultant* $\mathrm{Res}(P,Q)$ is defined as

$$\mathrm{Res}(P,Q) = \prod_{\alpha_i} Q(\alpha_i) = \prod_{\beta_j} P(\beta_j),$$

with $P(X) = \prod_{i=1}^{r}(X-\alpha_i)$ and $Q(X) = \prod_{j=1}^{s}(X-\beta_j)$.

For $P \in \mathbb{Z}[X]$, can we use the sequence of integers of the form $\mathrm{Res}(P, X^n-1)$ to find large primes?

~~Total~~ Quick Recall

- An *algebraic number* $\alpha \in \mathbb{C}$ is a root of a non-zero polynomial $P_\alpha(X) = \sum_{j=0}^{d_\alpha} a_j X^j \in \mathbb{Z}[X]$, such as $\sqrt{2}$, $\sqrt[3]{\frac{1}{2}}$.

~~Total~~ Quick Recall

- An *algebraic number* $\alpha \in \mathbb{C}$ is a root of a non-zero polynomial $P_\alpha(X) = \sum_{j=0}^{d_\alpha} a_j X^j \in \mathbb{Z}[X]$, such as $\sqrt{2}$, $\sqrt[3]{\frac{1}{2}}$.
- If such polynomial does not exist, then α is called a *transcendental number*, such as π.

~~Total~~ Quick Recall

- An *algebraic number* $\alpha \in \mathbb{C}$ is a root of a non-zero polynomial $P_\alpha(X) = \sum_{j=0}^{d_\alpha} a_j X^j \in \mathbb{Z}[X]$, such as $\sqrt{2}$, $\sqrt[3]{\frac{1}{2}}$.
- If such polynomial does not exist, then α is called a *transcendental number*, such as π.
- If $a_{d_\alpha} = 1$, then we call α an *algebraic integer*, such as $\sqrt{2}$.

~~Total~~ Quick Recall

- An *algebraic number* $\alpha \in \mathbb{C}$ is a root of a non-zero polynomial $P_\alpha(X) = \sum_{j=0}^{d_\alpha} a_j X^j \in \mathbb{Z}[X]$, such as $\sqrt{2}$, $\sqrt[3]{\frac{1}{2}}$.
- If such polynomial does not exist, then α is called a *transcendental number*, such as π.
- If $a_{d_\alpha} = 1$, then we call α an *algebraic integer*, such as $\sqrt{2}$.
- If $P_\alpha(X)$ cannot be factored into non-constant polynomials in $\mathbb{Z}[X]$ of degree $< \deg P_\alpha = d_\alpha$, then we call P_α is the *minimal polynomial* of α.

~~Total~~ Quick Recall II

- Consider $X^4 - 1$,

$$X^4 - 1 = (X-1)(X^3 + X^2 + X + 1) = (X-1)(X+1)[(X+i)(X-i)].$$

$\pm 1, \pm i$ are 4-th roots of unity, and they are the only ones.

~~Total~~ Quick Recall II

- Consider $X^4 - 1$,

$$X^4 - 1 = (X-1)(X^3+X^2+X+1) = (X-1)(X+1)[(X+i)(X-i)].$$

$\pm 1, \pm i$ are 4-th roots of unity, and they are the only ones.

- List of $d \mid 4$ is $\{1, 2, 4\}$. Minimal polynomial of $\zeta_1 = e^{\frac{2\pi i}{1}} = 1$ is $\phi_1(X) = (X-1)$, $\zeta_2 = e^{\frac{2\pi i}{2}} = -1$ is $\phi_2(X) = (X+1)$, and $\zeta_4 = e^{\frac{2\pi i}{4}} = i$ is $\phi_4(X) = X^2 + 1 = (X-i)(X+i)$.

~~Total~~ Quick Recall II

- Consider $X^4 - 1$,

$$X^4 - 1 = (X-1)(X^3 + X^2 + X + 1) = (X-1)(X+1)[(X+i)(X-i)].$$

$\pm 1, \pm i$ are 4-th roots of unity, and they are the only ones.

- List of $d \mid 4$ is $\{1, 2, 4\}$. Minimal polynomial of $\zeta_1 = e^{\frac{2\pi i}{1}} = 1$ is $\phi_1(X) = (X-1)$, $\zeta_2 = e^{\frac{2\pi i}{2}} = -1$ is $\phi_2(X) = (X+1)$, and $\zeta_4 = e^{\frac{2\pi i}{4}} = i$ is $\phi_4(X) = X^2 + 1 = (X-i)(X+i)$.

$$X^4 - 1 = \prod_{d|4} \phi_d(X).$$

~~Total~~ Quick Recall II

- Consider $X^4 - 1$,

$$X^4 - 1 = (X-1)(X^3 + X^2 + X + 1) = (X-1)(X+1)[(X+i)(X-i)].$$

$\pm 1, \pm i$ are 4-th roots of unity, and they are the only ones.

- List of $d \mid 4$ is $\{1, 2, 4\}$. Minimal polynomial of $\zeta_1 = e^{\frac{2\pi i}{1}} = 1$ is $\phi_1(X) = (X-1)$, $\zeta_2 = e^{\frac{2\pi i}{2}} = -1$ is $\phi_2(X) = (X+1)$, and $\zeta_4 = e^{\frac{2\pi i}{4}} = i$ is $\phi_4(X) = X^2 + 1 = (X-i)(X+i)$.

$$X^4 - 1 = \prod_{d|4} \phi_d(X).$$

- If α is a root of unity $\zeta_d^\ell = e^{\frac{2\pi i \ell}{d}}$ (such that $\gcd(\ell, d) = 1$), then the minimal polynomial is called the *d-th cyclotomic polynomial*, and denoted by $\phi_d(X)$.

A special sequence

- For $P \in \mathbb{Z}[X]$, T. Pierce (1918) and D. H. Lehmer (1932) considered $\mathrm{Res}(P, X^n - 1)$ to obtain large primes as its factors, they called it

$$\Delta_n(P) = \prod_{\alpha : P(\alpha)=0} (\alpha^n - 1).$$

A special sequence

- For $P \in \mathbb{Z}[X]$, T. Pierce (1918) and D. H. Lehmer (1932) considered $\mathrm{Res}(P, X^n - 1)$ to obtain large primes as its factors, they called it

$$\Delta_n(P) = \prod_{\alpha : P(\alpha)=0} (\alpha^n - 1).$$

- Regarding the sequence of integers Δ_n, Lehmer mentioned:

  " *These . . . are (one of) the best substitutes we have for actual formulas for prime numbers. Perhaps the most fundamental functions of this kind are special cases of* Δ_n" .

Why so special?

- Since $X^n - 1 = \prod_{d|n} \phi_d(X)$, where $\phi_d(X) \in \mathbb{Z}[X]$ is the *d-th cyclotomic polynomial*, we have

$$\Delta_n(P) = \prod_{\alpha:P(\alpha)=0} \prod_{d|n} \phi_d(\alpha)$$

Why so special?

- Since $X^n - 1 = \prod_{d|n} \phi_d(X)$, where $\phi_d(X) \in \mathbb{Z}[X]$ is the *d-th cyclotomic polynomial*, we have

$$\Delta_n(P) = \prod_{\alpha : P(\alpha)=0} \prod_{d|n} \phi_d(\alpha) = \prod_{d|n} \left(\prod_{\alpha : P(\alpha)=0} \phi_d(\alpha) \right) = \prod_{d|n} \mathrm{Res}(P, \phi_d).$$

Why so special?

- Since $X^n - 1 = \prod_{d|n} \phi_d(X)$, where $\phi_d(X) \in \mathbb{Z}[X]$ is the *d-th cyclotomic polynomial*, we have

$$\Delta_n(P) = \prod_{\alpha : P(\alpha)=0} \prod_{d|n} \phi_d(\alpha) = \prod_{d|n} \left(\prod_{\alpha : P(\alpha)=0} \phi_d(\alpha) \right) = \prod_{d|n} \mathrm{Res}(P, \phi_d).$$

- Given complete factorization of $\Delta_d(P)$ for $d \mid n, d < n$, the *essential factor* is $\mathrm{Res}(P, \phi_n)$.

Why so special?

- Since $X^n - 1 = \prod_{d|n} \phi_d(X)$, where $\phi_d(X) \in \mathbb{Z}[X]$ is the *d-th cyclotomic polynomial*, we have

$$\Delta_n(P) = \prod_{\alpha : P(\alpha)=0} \prod_{d|n} \phi_d(\alpha) = \prod_{d|n} \left(\prod_{\alpha : P(\alpha)=0} \phi_d(\alpha) \right) = \prod_{d|n} \mathrm{Res}(P, \phi_d).$$

- Given complete factorization of $\Delta_d(P)$ for $d \mid n, d < n$, the *essential factor* is $\mathrm{Res}(P, \phi_n)$.
- The *characteristic prime factors* q of $\Delta_n(P)$ are all primes $q \nmid \Delta_d(P)$. $\mathrm{Res}(P, \phi_n)$ contains all these q.
- $q \nmid n$.

Why so special?

- Since $X^n - 1 = \prod_{d|n} \phi_d(X)$, where $\phi_d(X) \in \mathbb{Z}[X]$ is the *d-th cyclotomic polynomial*, we have

$$\Delta_n(P) = \prod_{\alpha:P(\alpha)=0} \prod_{d|n} \phi_d(\alpha) = \prod_{d|n} \left(\prod_{\alpha:P(\alpha)=0} \phi_d(\alpha) \right) = \prod_{d|n} \mathrm{Res}(P, \phi_d).$$

- Given complete factorization of $\Delta_d(P)$ for $d \mid n, d < n$, the *essential factor* is $\mathrm{Res}(P, \phi_n)$.
- The *characteristic prime factors* q of $\Delta_n(P)$ are all primes $q \nmid \Delta_d(P)$. $\mathrm{Res}(P, \phi_n)$ contains all these q.
- $q \nmid n$.

Moral of the story: Follow "Mersenne-strategy", and restrict to $n = p$ primes and irreducible polynomials P.

Some more properties

Some more properties

- $\Delta_n(P)$ satisfies recurrence relation.
- $\Delta_n(P)$ is periodic of period m (i.e. $\{\Delta_n(P) : n \geq 1\}$ has exactly m distinct integers) if and only if $P(X) = \phi_m(X)$.
- Then $\Delta_n(P)$ is either 0 or 1 or some prime power ℓ^k, $\ell \mid m, \ell \nmid n$.

Some more properties

- $\Delta_n(P)$ satisfies recurrence relation.
- $\Delta_n(P)$ is periodic of period m (i.e. $\{\Delta_n(P) : n \geq 1\}$ has exactly m distinct integers) if and only if $P(X) = \phi_m(X)$.
- Then $\Delta_n(P)$ is either 0 or 1 or some prime power ℓ^k, $\ell \mid m, \ell \nmid n$.
- For P non-cyclotomic polynomial, $|\Delta_n(P)|$ is unbounded as n grows.

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(P)}{\Delta_n(P)} \right| = \prod_{\alpha : P(\alpha)=0} \max\{1, |\alpha|\} =: M(P).$$

Some more properties

- $\Delta_n(P)$ satisfies recurrence relation.
- $\Delta_n(P)$ is periodic of period m (i.e. $\{\Delta_n(P) : n \geq 1\}$ has exactly m distinct integers) if and only if $P(X) = \phi_m(X)$.
- Then $\Delta_n(P)$ is either 0 or 1 or some prime power ℓ^k, $\ell \mid m, \ell \nmid n$.
- For P non-cyclotomic polynomial, $|\Delta_n(P)|$ is unbounded as n grows.

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(P)}{\Delta_n(P)} \right| = \prod_{\alpha : P(\alpha)=0} \max\{1, |\alpha|\} =: M(P).$$

- For characteristic prime factors q_n, $q_n^{e(n)} \mid\mid \Delta_n(P)$, the $e(n)$ increases with n.

Some more properties

- $\Delta_n(P)$ satisfies recurrence relation.
- $\Delta_n(P)$ is periodic of period m (i.e. $\{\Delta_n(P) : n \geq 1\}$ has exactly m distinct integers) if and only if $P(X) = \phi_m(X)$.
- Then $\Delta_n(P)$ is either 0 or 1 or some prime power ℓ^k, $\ell \mid m, \ell \nmid n$.
- For P non-cyclotomic polynomial, $|\Delta_n(P)|$ is unbounded as n grows.

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}(P)}{\Delta_n(P)} \right| = \prod_{\alpha : P(\alpha)=0} \max\{1, |\alpha|\} =: M(P).$$

- For characteristic prime factors q_n, $q_n^{e(n)} \mid\mid \Delta_n(P)$, the $e(n)$ increases with n.

ADVANTAGE: The sequence $\{\Delta_n(P) : n \geq 1\}$ does not increase rapidly when $M(P)$ is smaller.

How small can $M(P)$ be?

Consider a non-zero polynomial $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{Z}[X]$.

How small can $M(P)$ be?

Consider a non-zero polynomial $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{Z}[X]$.

- $M(P) = \prod_{j=1}^{d} \max\{1, |\alpha_j|\} \geq 1$.

How small can $M(P)$ be?

Consider a non-zero polynomial $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{Z}[X]$.

- $M(P) = \prod_{j=1}^{d} \max\{1, |\alpha_j|\} \geq 1$.
- $P(0) \neq 0$ and $M(P) = 1$ if and only if $P(X) = \prod_k \phi_k(X)$. (Kronecker's Theorem)
- This implies that $\Delta_n(P)$ is periodic when $M(P) = 1$.

How small can $M(P)$ be?

Consider a non-zero polynomial $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{Z}[X]$.

- $M(P) = \prod_{j=1}^{d} \max\{1, |\alpha_j|\} \geq 1$.
- $P(0) \neq 0$ and $M(P) = 1$ if and only if $P(X) = \prod_k \phi_k(X)$. (Kronecker's Theorem)
- This implies that $\Delta_n(P)$ is periodic when $M(P) = 1$.

Lehmer's question

Does there exists a $C > 1$, such that $M(P) \geq C$ for all non-cyclotomic polynomials?

Lower bound for $M(P)$?

A *reciprocal/symmetric polynomial* P of degree d is a polynomial satisfying $P(X) = X^d P\left(\frac{1}{X}\right)$.

Lower bound for $M(P)$?

A *reciprocal/symmetric polynomial* P of degree d is a polynomial satisfying $P(X) = X^d P\left(\frac{1}{X}\right)$.

- For P reciprocal, $\left|\frac{\Delta_p(P)}{\Delta_1(P)}\right|$ is a square, for odd primes p. It is better to consider $\sqrt{\left|\frac{\Delta_p(P)}{\Delta_1(P)}\right|}$.

Lower bound for $M(P)$?

A *reciprocal/symmetric polynomial* P of degree d is a polynomial satisfying $P(X) = X^d P\left(\frac{1}{X}\right)$.

- For P reciprocal, $\left|\frac{\Delta_p(P)}{\Delta_1(P)}\right|$ is a square, for odd primes p. It is better to consider $\sqrt{\left|\frac{\Delta_p(P)}{\Delta_1(P)}\right|}$.
- Lehmer-Poulet (1932): For

$$P(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1,$$

$M(P) = 1.17628081\ldots$, and

$$\sqrt{\left|\frac{\Delta_{379}(P)}{\Delta_1(P)}\right|} = 1{,}794{,}327{,}140{,}357 \quad \text{is a prime.}$$

Lower bound contd.

- If P is irreducible and non-reciprocal, then Smyth (1971) showed $M(P) \geq M(X^3 - X - 1) = 1.32471795\ldots$.

Lower bound contd.

- If P is irreducible and non-reciprocal, then Smyth (1971) showed $M(P) \geq M(X^3 - X - 1) = 1.32471795\ldots$.
- If P is irreducible and non-cyclotomic of degree d, then Dobrowolski (1979) showed

$$M(P) \geq 1 + c\left(\frac{\log\log d}{\log d}\right)^3.$$

Lower bound contd.

- If P is irreducible and non-reciprocal, then Smyth (1971) showed $M(P) \geq M(X^3 - X - 1) = 1.32471795\ldots$.
- If P is irreducible and non-cyclotomic of degree d, then Dobrowolski (1979) showed

$$M(P) \geq 1 + c\left(\frac{\log\log d}{\log d}\right)^3.$$

- Dimitrov (2019): For irreducible monic polynomials P of degree d,

$$\max\{|\alpha| : P(\alpha) = 0\} \geq 2^{\frac{1}{4d}},$$

so $M(P)$ cannot be too small.

Lower bound contd.

- If P is irreducible and non-reciprocal, then Smyth (1971) showed $M(P) \geq M(X^3 - X - 1) = 1.32471795\ldots$.
- If P is irreducible and non-cyclotomic of degree d, then Dobrowolski (1979) showed

$$M(P) \geq 1 + c\left(\frac{\log\log d}{\log d}\right)^3.$$

- Dimitrov (2019): For irreducible monic polynomials P of degree d,

$$\max\{|\alpha| : P(\alpha) = 0\} \geq 2^{\frac{1}{4d}},$$

so $M(P)$ cannot be too small.

Lehmer's question is still open. The smallest known value of $M(P)$ is still due to Lehmer and Poulet.

David Boyd's approach

One of the most interesting attempts towards the resolution of Lehmer's question has been given by David W. Boyd in 1981. He considered

$$\mathcal{M} = \{M(P) : P(X) \in \mathbb{Z}[X] \setminus \{0\}\}.$$

David Boyd's approach

One of the most interesting attempts towards the resolution of Lehmer's question has been given by David W. Boyd in 1981. He considered

$$\mathcal{M} = \{M(P) : P(X) \in \mathbb{Z}[X] \setminus \{0\}\}.$$

- $\mathcal{M}$ is a countable set of algebraic numbers in $[1, \infty)$, and a semigroup under multiplication $M(PQ) = M(P)M(Q)$.

David Boyd's approach

One of the most interesting attempts towards the resolution of Lehmer's question has been given by David W. Boyd in 1981. He considered

$$\mathcal{M} = \{M(P) : P(X) \in \mathbb{Z}[X] \setminus \{0\}\}.$$

- $\mathcal{M}$ is a countable set of algebraic numbers in $[1, \infty)$, and a semigroup under multiplication $M(PQ) = M(P)M(Q)$.
- Lehmer's question is equivalent to asking

  Is 1 an isolated limit point of $\mathcal{M}$?

David Boyd's approach

One of the most interesting attempts towards the resolution of Lehmer's question has been given by David W. Boyd in 1981. He considered

$$\mathcal{M} = \{M(P) : P(X) \in \mathbb{Z}[X] \setminus \{0\}\}.$$

- $\mathcal{M}$ is a countable set of algebraic numbers in $[1, \infty)$, and a semigroup under multiplication $M(PQ) = M(P)M(Q)$.
- Lehmer's question is equivalent to asking

  Is 1 an isolated limit point of $\mathcal{M}$?

- If $\mathcal{M}$ is a closed subset of $[1, \infty)$, then $\mathcal{M}$ is nowhere dense, and hence 1 *is* an isolated limit point.

David Boyd's approach

One of the most interesting attempts towards the resolution of Lehmer's question has been given by David W. Boyd in 1981. He considered

$$\mathcal{M} = \{M(P) : P(X) \in \mathbb{Z}[X] \setminus \{0\}\}.$$

- $\mathcal{M}$ is a countable set of algebraic numbers in $[1, \infty)$, and a semigroup under multiplication $M(PQ) = M(P)M(Q)$.
- Lehmer's question is equivalent to asking

  Is 1 an isolated limit point of $\mathcal{M}$?

- If $\mathcal{M}$ is a closed subset of $[1, \infty)$, then $\mathcal{M}$ is nowhere dense, and hence 1 *is* an isolated limit point.
- Unfortunately, it is improbable that $\mathcal{M}$ is closed, as the closure of $\mathcal{M}$ may contain "special" *transcendental numbers*.

Staring at the closure

To determine the closure, we need a generalization and a theorem.

$$\mathbb{T}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^\times \times \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times : |x_1| = \cdots = |x_n| = 1\}.$$

Staring at the closure

To determine the closure, we need a generalization and a theorem.

$$\mathbb{T}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^\times \times \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times : |x_1| = \cdots = |x_n| = 1\}.$$

- For $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{C}[X]$,

$$\log M(P) = \sum_{j=1}^{d} \log \max\{1, |\alpha_j|\} = \frac{1}{2\pi i}\int_{\mathbb{T}^1} \log|P(X)| \frac{dX}{X}.$$

Staring at the closure

To determine the closure, we need a generalization and a theorem.

$$\mathbb{T}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^\times \times \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times : |x_1| = \cdots = |x_n| = 1\}.$$

- For $P(X) = \prod_{j=1}^{d}(X - \alpha_j) \in \mathbb{C}[X]$,

$$\log M(P) = \sum_{j=1}^{d} \log\max\{1, |\alpha_j|\} = \frac{1}{2\pi i}\int_{\mathbb{T}^1} \log|P(X)|\frac{dX}{X}.$$

Definition

For $Q \in \mathbb{C}[x_1, \ldots, x_n]$, the *logarithmic Mahler measure* of Q is defined as

$$\log M(Q) = \mathrm{m}(Q) := \frac{1}{(2\pi i)^n}\int_{\mathbb{T}^n} \log|Q(x_1, \ldots, x_n)|\frac{dx_1}{x_1}\cdots\frac{dx_n}{x_n}.$$

Staring at the closure

To determine the closure, we need a generalization and a theorem.

$$\mathbb{T}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^\times \times \mathbb{C}^\times \times \cdots \times \mathbb{C}^\times : |x_1| = \cdots = |x_n| = 1\}.$$

- For $P(X) = \prod_{j=1}^d (X - \alpha_j) \in \mathbb{C}[X]$,

$$\log M(P) = \sum_{j=1}^{d} \log \max\{1, |\alpha_j|\} = \frac{1}{2\pi i} \int_{\mathbb{T}^1} \log |P(X)| \frac{dX}{X}.$$

Definition

For $Q \in \mathbb{C}[x_1, \ldots, x_n]$, the *logarithmic Mahler measure* of Q is defined as

$$\log M(Q) = \mathrm{m}(Q) := \frac{1}{(2\pi i)^n} \int_{\mathbb{T}^n} \log |Q(x_1, \ldots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}.$$

It first appeared in a proof of Gelfond's inequality by Kurt Mahler (1962) involving a certain height of polynomials.

Still staring

Consider

$$\mathcal{M}_n = \{M(Q) : Q \in \mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}\}.$$

Still staring

Consider

$$\mathcal{M}_n = \{M(Q) : Q \in \mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}\}.$$

- Boyd-Lawton (1983): For $Q \in \mathbb{C}[x_1, \ldots, x_n]$,

$$\lim_{m_2 \to \infty} \cdots \lim_{m_n \to \infty} \mathrm{m}(Q(x_1, x_1^{m_2}, \ldots, x_1^{m_n})) = \mathrm{m}(Q(x_1, x_2, \ldots, x_n)).$$

Still staring

Consider

$$\mathcal{M}_n = \{M(Q) : Q \in \mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}\}.$$

- Boyd-Lawton (1983): For $Q \in \mathbb{C}[x_1, \ldots, x_n]$,

$$\lim_{m_2 \to \infty} \cdots \lim_{m_n \to \infty} \mathrm{m}(Q(x_1, x_1^{m_2}, \ldots, x_1^{m_n})) = \mathrm{m}(Q(x_1, x_2, \ldots, x_n)).$$

- $\mathcal{M}_1 = \mathcal{M} \subseteq \mathcal{M}_n \subseteq \mathcal{M}_{n+1}$, for all $n \geq 1$.
- $\mathcal{M}_n$ are countable subsets of $[1, \infty)$, and are subsets of the set of limit points of $\mathcal{M}_1$.

Still staring

Consider

$$\mathcal{M}_n = \{M(Q) : Q \in \mathbb{C}[x_1, \dots, x_n] \setminus \{0\}\}.$$

- Boyd-Lawton (1983): For $Q \in \mathbb{C}[x_1, \dots, x_n]$,

$$\lim_{m_2 \to \infty} \cdots \lim_{m_n \to \infty} \mathrm{m}(Q(x_1, x_1^{m_2}, \dots, x_1^{m_n})) = \mathrm{m}(Q(x_1, x_2, \dots, x_n)).$$

- $\mathcal{M}_1 = \mathcal{M} \subseteq \mathcal{M}_n \subseteq \mathcal{M}_{n+1}$, for all $n \geq 1$.
- $\mathcal{M}_n$ are countable subsets of $[1, \infty)$, and are subsets of the set of limit points of $\mathcal{M}_1$.
- Boyd's Conjecture: $\bigcup_{n \geq 1} \mathcal{M}_n$ is closed in $[1, \infty)$, and hence nowhere dense.
- This would give an affirmative answer to Lehmer's question.

Quick detour

- *Riemann ζ-function*:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \qquad \text{for } \mathrm{Re}(s) > 1.$$

$\zeta(2) = \frac{\pi^2}{6}$, $\zeta(3) = 1.202056903\ldots$ is irrational (Apéry).

Quick detour

- *Riemann ζ-function*:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \qquad \text{for } \mathrm{Re}(s) > 1.$$

$\zeta(2) = \frac{\pi^2}{6}$, $\zeta(3) = 1.202056903\ldots$ is irrational (Apéry).

- *L-function* an arithmetic "object" X expressed as

$$L(X, s) = \sum_{n \geq 1} \frac{a_n(X)}{n^s} \qquad \text{for } \mathrm{Re}(s) > \sigma,$$

where $a_n(X)$ are complex numbers associated to X. X can be Dirichlet characters, elliptic curves, etc.

Quick detour

- *Riemann ζ-function*:

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} \qquad \text{for } \mathrm{Re}(s) > 1.$$

$\zeta(2) = \frac{\pi^2}{6}$, $\zeta(3) = 1.202056903\ldots$ is irrational (Apéry).

- *L-function* an arithmetic "object" X expressed as

$$L(X, s) = \sum_{n\geq 1} \frac{a_n(X)}{n^s} \qquad \text{for } \mathrm{Re}(s) > \sigma,$$

where $a_n(X)$ are complex numbers associated to X. X can be Dirichlet characters, elliptic curves, etc.

- Special values of $L(X, s)$ and (logarithmic) Mahler measure belong to a set of special kinds of numbers called *periods*,

Quick detour

- *Riemann ζ-function*:

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} \qquad \text{for } \mathrm{Re}(s) > 1.$$

$\zeta(2) = \frac{\pi^2}{6}$, $\zeta(3) = 1.202056903\ldots$ is irrational (Apéry).

- *L-function* an arithmetic "object" X expressed as

$$L(X, s) = \sum_{n\geq 1} \frac{a_n(X)}{n^s} \qquad \text{for } \mathrm{Re}(s) > \sigma,$$

where $a_n(X)$ are complex numbers associated to X. X can be Dirichlet characters, elliptic curves, etc.

- Special values of $L(X, s)$ and (logarithmic) Mahler measure belong to a set of special kinds of numbers called *periods*, which have applications in transcendental number theory and algebraic geometry.

What numbers appear in $\log \mathcal{M}_n$?

- Smyth (1981): $\mathrm{m}(1 + x + y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2)$.

What numbers appear in $\log \mathcal{M}_n$?

- Smyth (1981): $\mathrm{m}(1+x+y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2)$.
- Smyth, Boyd (1981): $\mathrm{m}(1+x+y+z) = \frac{7}{2\pi^2}\zeta(3)$.

What numbers appear in $\log \mathcal{M}_n$?

- Smyth (1981): $\mathrm{m}(1 + x + y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2)$.
- Smyth, Boyd (1981): $\mathrm{m}(1 + x + y + z) = \frac{7}{2\pi^2}\zeta(3)$.
- Deninger (1996): $\mathrm{m}(P)$ as certain integral of a differential n-form over a algebraic n-cycle, and conjectured

$$\mathrm{m}\left(x + \frac{1}{x} + y + \frac{1}{y} + 1\right) \stackrel{?}{=} \frac{15}{4\pi^2} L(E_{15}, 2),$$

later proved by Rogers-Zudilin (2010).

What numbers appear in $\log \mathcal{M}_n$?

- Smyth (1981): $\mathrm{m}(1+x+y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2)$.
- Smyth, Boyd (1981): $\mathrm{m}(1+x+y+z) = \frac{7}{2\pi^2}\zeta(3)$.
- Deninger (1996): $\mathrm{m}(P)$ as certain integral of a differential n-form over a algebraic n-cycle, and conjectured

$$\mathrm{m}\left(x + \frac{1}{x} + y + \frac{1}{y} + 1\right) \stackrel{?}{=} \frac{15}{4\pi^2} L(E_{15}, 2),$$

  later proved by Rogers-Zudilin (2010).
- Boyd (1998): For some families of polynomials $P_k(x,y)$, with parameter k,

$$\mathrm{m}(P_k) \stackrel{?}{=} \frac{r_k N(k)}{4\pi^2} L(E_{N(k)}, 2),$$

  where $k^2 \in \mathbb{Z}$, $r_k \in \mathbb{Q}$ and $E_{N(k)}$ is an elliptic curve associated to the polynomial P_k.

Examples contd.

- Rodriguez-Villegas (1997): Proved Boyd's conjecture for

$$Q_k := Q_k(x,y) = x + \frac{1}{x} + y + \frac{1}{y} + k,$$

when $k = 2\sqrt{2}, 4\sqrt{2}$.

Examples contd.

- Rodriguez-Villegas (1997): Proved Boyd's conjecture for

$$Q_k := Q_k(x,y) = x + \frac{1}{x} + y + \frac{1}{y} + k,$$

  when $k = 2\sqrt{2}, 4\sqrt{2}$.
- Lalín (2010): Proved Boyd's conjecture for $k = 5$.
- Brunault (2015): Proved Boyd's conjecture for $k = 12$.

Generalized Mahler measure

In a different direction, Cassaigne-Maillot (2000) generalized the result of Smyth (1981), and explicitly computed $\mathrm{m}(ax + by + c)$ in terms of the volume of a certain hyperbolic triangle depending on $|a|$, $|b|$ and $|c|$, for $a, b, c \in \mathbb{C}^*$.

Generalized Mahler measure

In a different direction, Cassaigne-Maillot (2000) generalized the result of Smyth (1981), and explicitly computed $\mathrm{m}(ax + by + c)$ in terms of the volume of a certain hyperbolic triangle depending on $|a|, |b|$ and $|c|$, for $a, b, c \in \mathbb{C}^*$.

Definition

The *generalized Mahler measure* of a Laurent polynomial $P \in \mathbb{C}(x_1, \ldots, x_n)^*$ is defined as

$$\mathrm{m}_{a_1,\ldots,a_n}(P) := \frac{1}{(2\pi \mathrm{i})^n} \int_{\mathbb{T}^n_{\mathbf{a}}} \log |P(x_1, \ldots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n},$$

where $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n_{>0}$ and

$$\mathbb{T}^n_{\mathbf{a}} := \{(x_1, \ldots, x_n) \in \mathbb{C}^* \times \mathbb{C}^* \times \cdots \times \mathbb{C}^* : |x_1| = a_1, \ldots, |x_n| = a_n\}.$$

Result

Recall the family $Q_k(x,y) = x + \frac{1}{x} + y + \frac{1}{y} + k$, and consider

$$\mathbb{T}^2_{a,b} = \{(x,y) \in \mathbb{C}^\times \times \mathbb{C}^\times : |x| = a, |y| = b\}.$$

Result

Recall the family $Q_k(x,y) = x + \frac{1}{x} + y + \frac{1}{y} + k$, and consider

$$\mathbb{T}^2_{a,b} = \{(x,y) \in \mathbb{C}^\times \times \mathbb{C}^\times : |x| = a, |y| = b\}.$$

- R.(2024): Given $a, b > 0$, if $Q_k(x,y) \neq 0$ for any $(x,y) \in \mathbb{T}^2_{a,b}$, then

$$\mathrm{m}_{a,b}(Q_k) = \mathrm{m}(Q_k(ax, by)) = \mathrm{m}(Q_k) \quad \text{or} \quad \max\{\log a, \log b\}.$$

Result

Recall the family $Q_k(x,y) = x + \frac{1}{x} + y + \frac{1}{y} + k$, and consider

$$\mathbb{T}^2_{a,b} = \{(x,y) \in \mathbb{C}^\times \times \mathbb{C}^\times : |x| = a, |y| = b\}.$$

- R.(2024): Given $a, b > 0$, if $Q_k(x,y) \neq 0$ for any $(x,y) \in \mathbb{T}^2_{a,b}$, then

$$\mathrm{m}_{a,b}(Q_k) = \mathrm{m}(Q_k(ax, by)) = \mathrm{m}(Q_k) \quad \text{or} \quad \max\{\log a, \log b\}.$$

- This shows that, under the non-vanishing condition, shrinking or extending the integration torus either does not change the Mahler measure or the change is linear.

contd.

- This provides evidence for Boyd's conjecture of a large number of polynomials. For example, for $a \in \left(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\right)$,

$$\mathrm{m}_{a,a}(Q_{2i}) = \mathrm{m}_{a,\sqrt{a}}(Q_{2i}) = \mathrm{m}(Q_{2i}) = \frac{40}{4\pi^2} L(E_{40}, 2),$$

where the last equality is due to Mellit (2011).

contd.

- This provides evidence for Boyd's conjecture of a large number of polynomials. For example, for $a \in \left(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\right)$,

$$\mathrm{m}_{a,a}(Q_{2i}) = \mathrm{m}_{a,\sqrt{a}}(Q_{2i}) = \mathrm{m}(Q_{2i}) = \frac{40}{4\pi^2} L(E_{40}, 2),$$

  where the last equality is due to Mellit (2011).

- Similar methodology of the proof extends the result for any n-variable polynomial with complex coefficients.

contd.

- This provides evidence for Boyd's conjecture of a large number of polynomials. For example, for $a \in \left(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\right)$,

$$\mathrm{m}_{a,a}(Q_{2i}) = \mathrm{m}_{a,\sqrt{a}}(Q_{2i}) = \mathrm{m}(Q_{2i}) = \frac{40}{4\pi^2} L(E_{40}, 2),$$

  where the last equality is due to Mellit (2011).

- Similar methodology of the proof extends the result for any n-variable polynomial with complex coefficients.

- R. (2024): explicit expression of $\mathrm{m}_{a,b}(Q_4)$ in terms of hyperbolic volumes for all $a, b > 0$.

Some final destinations

- Boyd's conjectures are far from being proved completely. Some methodologies that appeared in different proofs involve machinery from Modular forms, arithmetic properties of objects from Algebraic geometry (such as cohomologies associated with varieties).

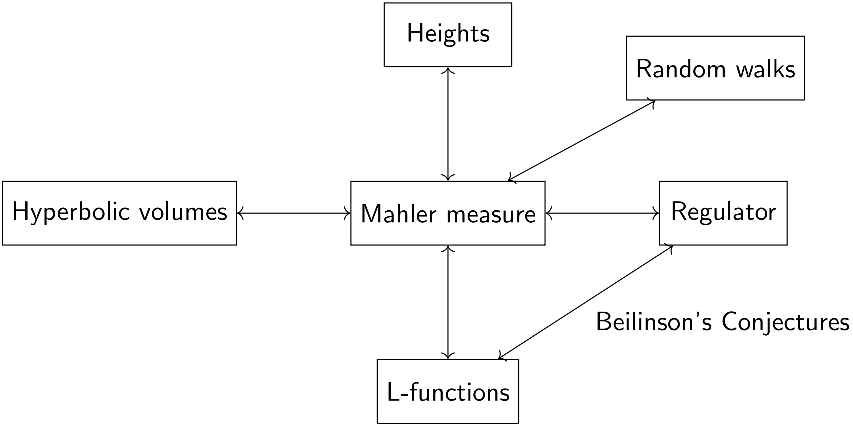
Some final destinations

- Boyd's conjectures are far from being proved completely. Some methodologies that appeared in different proofs involve machinery from Modular forms, arithmetic properties of objects from Algebraic geometry (such as cohomologies associated with varieties).
- Mahler measures are also considered as certain height functions of polynomials or varieties defined by polynomials. Different generalizations of Mahler measures are considered based on this fact, such as *Dynamical Mahler measure* etc.

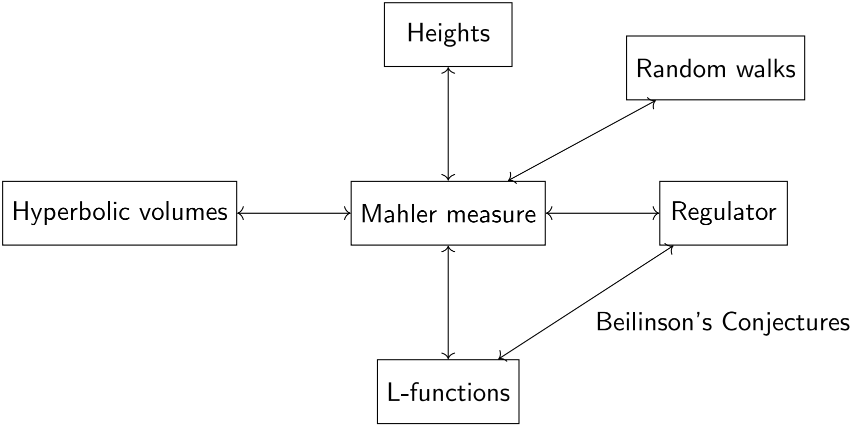
Some final destinations

- Boyd's conjectures are far from being proved completely. Some methodologies that appeared in different proofs involve machinery from Modular forms, arithmetic properties of objects from Algebraic geometry (such as cohomologies associated with varieties).
- Mahler measures are also considered as certain height functions of polynomials or varieties defined by polynomials. Different generalizations of Mahler measures are considered based on this fact, such as *Dynamical Mahler measure* etc.
- Certain changes of the integration domain, affect the Mahler measure significantly. For example, replacing unit torus by unit disc results in a negative answer for Lehmer's question in the respective setting.

Mahler measure, a symphony!



Mahler measure, a symphony!



A symphony must be like the world. It must contain everything.

— Gustav Mahler.

Thank you for your attention!