European Research Council
Established by
the European Commission

The least common multiple of polynomial sequences

Cetraro, July 2019

Zeev Rudnick, TAU

Question: $\mathrm{LCM}(1,2,\ldots,N) =?$

Given integers $a_1, \ldots, a_N$, the **least common multiple** $L(N) \coloneqq \mathrm{lcm}\,(a_1, \ldots, a_N)$ is uniquely defined (up to sign) by requiring

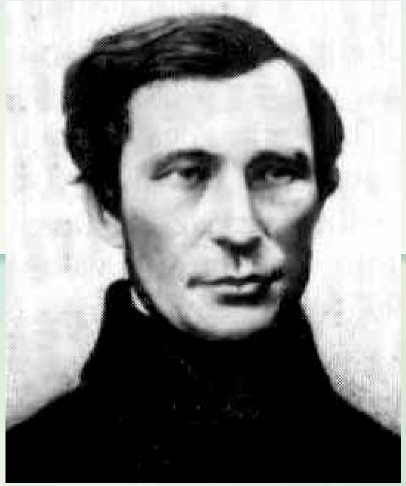
- L is a common multiple: $a_i \mid L, \ \ \forall\, i$
- L is minimal: If $a_i \mid L' \quad \forall\, i$ then $L \mid L'$.

Example: $\mathrm{LCM}(60,378,75) = \mathrm{LCM}\left(2^2 \cdot 3 \cdot 5,\ 2 \cdot 3^3 \cdot 7,\ 3 \cdot 5^2\right) = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7$

Some properties of LCM's:

- $\mathrm{lcm}(a,b) = ab/\mathrm{gcd}(a,b)$
- For p prime, $\mathrm{lcm}\,(p^{k_1}, \ldots, p^{k_N}) = p^{\max k_i}$
- $\mathrm{lcm}(a_1,\ldots,a_N) = \prod_p p^{\max(\nu_p(a_i):\quad i=1,\ldots,N)}$
- Recursion: $\mathrm{lcm}(a_1, a_2, \ldots, a_N) = \mathrm{lcm}(\mathrm{lcm}(a_1, a_2), a_3, \ldots, a_N)$
- Complexity: quadratic in N and in $\max \log a_i$.

Chebyshev



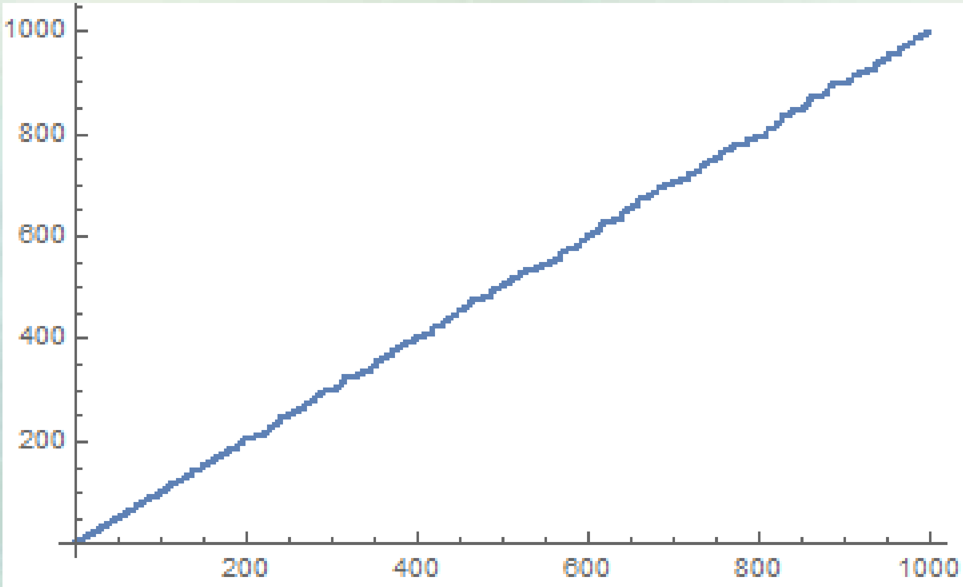
Exercise: $\log \mathrm{LCM}(1,2,\ldots,N) = \psi(N)$

$$\psi(N) := \sum_{n\le N} \Lambda(n) = \sum_{p,k\ge 1,\, p^k \le N} \log p$$

Chebyshev (1850): $0.9 \cdot \mathrm{N} < \psi(N) < 1.11 \cdot N$

Prime Number Theorem (1890's): $\psi(N) \sim N$

$$\mathrm{PNT} \quad \Leftrightarrow \quad \log \mathrm{LCM}(1,\ldots,N) \sim N$$



Plot of $\log \mathrm{LCM}(1,2,\ldots,N)$, $N \le 1000$

Cilleruelo's conjecture

Javier Cilleruelo (1961-2016)

What can we say about the LCM of a sequence of polynomial values?
For $f \in \boldsymbol{Z}[x]$, let

$$L_f(N) := \mathrm{lcm}\,(\ f(1), \ldots, f(N)\ )$$

For f split /Q $f(x) = \prod(a_i x + b_i)$, it is easy to see from Chebyshev that

$$\log L_f(N) \sim c_f\, N$$

for instance, if $f(x) = x(x+1)$ then $c_f = 1$.

Cilleruelo conjectured that if f is **<u>irreducible</u>** of degree $d \geq 2$, then $\log L_f(N)$ grows faster:

$$\log L_f(N) \sim (d-1) N \log N, \qquad N \to \infty$$

What’s known for general f(x)

Upper bound: For any f, $\log L_f(N) \ll N \log N$

Lower bound (ZR and James Maynard, December 2018): If f is not split /Q then $\log L_f(N) \gg N \log N$

-Previous lower bound $\log L_f(N) \gg N$ for f with non-negative coefficients (Hong, Luo, Qian & Wang 2013)

Thus if f is not split, then we have an analogue of Chebyshev's theorem towards the PNT!

$$N \log N \ll \log L_f(N) \ll N \log N$$

A lower bound (ZR & J Maynard): $\log L_f(N) \gg N \log N$

We use a result (``Chebyshev's problem") on the largest prime factor $P_+(f(n))$ of $f(n)$

T. Nagell (1921): Let $f \in \boldsymbol{Z}[x]$ be irreducible of degree $d \geq 2$. Then there is a set S of **positive density** of n's s.t.

$$P_+\big(f(n)\big) \geq n(\log n)^{\frac{1}{2}}, \quad \forall n \in S$$

- further work by Erdos 1952, Tennenbaum 1990.

- $P_+(f(n)) > n^{1+\vartheta}$ (for a set of positive density) by Hooley (1967) for $f(x) = x^2 + D$ and by Deshouillers & Iwaniec;
- Heath Brown (2001) $f(x) = x^3 + 2$, see also Dartyge 2015, de la Bretèche 2015, Irving 2015…

Pretending that these primes $P_+\big(f(n)\big), n \in S,$ are **distinct*** implies that their product certainly divides $L_f(N)$ $= \mathrm{LCM}(f(1), f(2), \dots, f(N))$, and hence

$$\log L_f(N) \geq \sum_{n \leq N, n \in S} \log P_+(f(n)) \geq \sum_{n \leq N, n \in S} \log\Big(N\sqrt{\log N}\Big) \geq \#\{n \in S \quad, n \leq N\} \times \log N$$

Since $\#\{n \in S: n \leq N\} \geq cN$ (S has positive density), we deduce that $\log L_f(N) \gg N \log N$

*not strictly true, substitute needs $P_+\big(f(n)\big) \gg n$.

The quadratic case

Cilleruelo (2011) : If f is **irreducible** and $\mathbf{deg}\, \boldsymbol{f} = \mathbf{2}$, then $\log L_f(N) \sim N \log N$

Moreover, there is a secondary term $\log L_f(N) = N \log N + B_f\, N + o(N)$

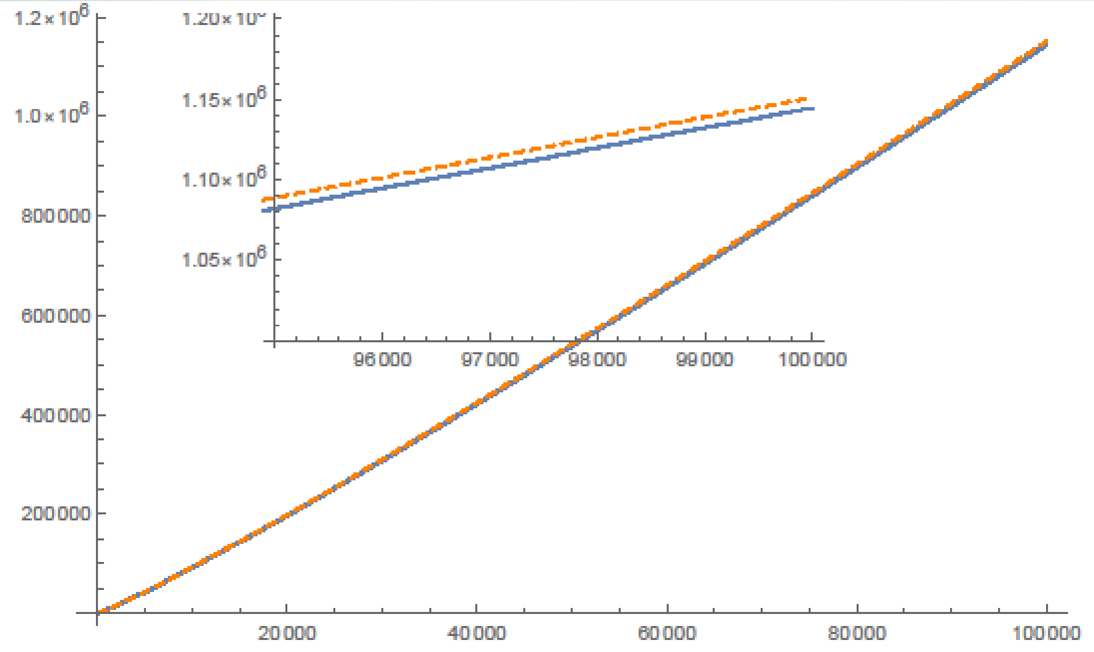
To get the secondary term, uses uniform distribution of solutions of quadratic congruences modulo p (Duke, Friedlander & Iwaniec 1995, Toth 2000).

e.g. for $f(x) = x^2 + 1$, $$B_f = \gamma - 1 - \frac{\log 2}{2} - \sum_{p \neq 2} \frac{\left(\frac{-1}{p}\right) \log p}{p - 1} \approx -0.066275634$$

Rué, Šarka and Zumalacárregui (2013): for $f(x) = x^2 + 1$, give remainder $O(N/(\log N)^{4/9})$

Numerics for $f(x) = x^2 + 1$

$$L_f(N) \coloneqq \mathrm{LCM}(f(1), f(2), \ldots, f(N))$$



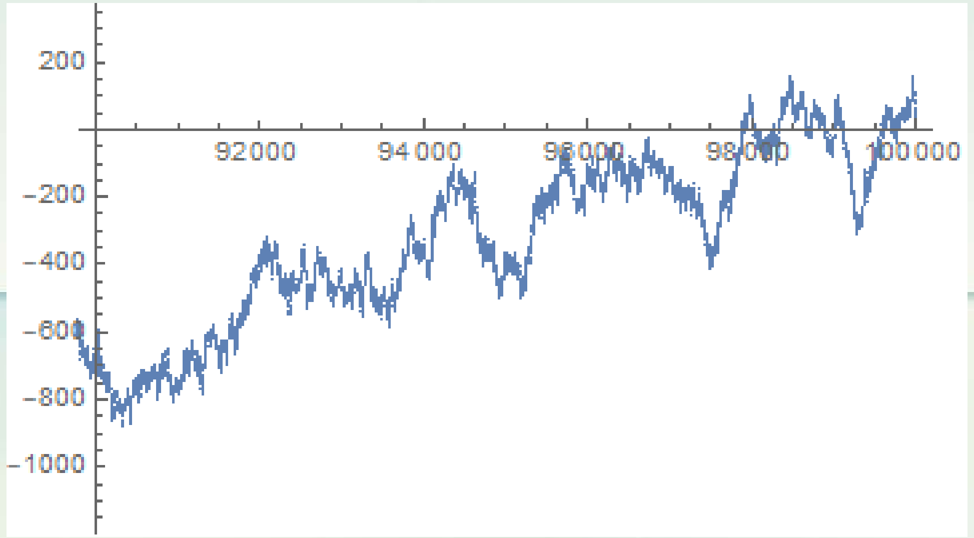
$\log L_f(N)$ (solid) vs. $N \log N$ -----, N<100,000

Inset: 95000<N<100000

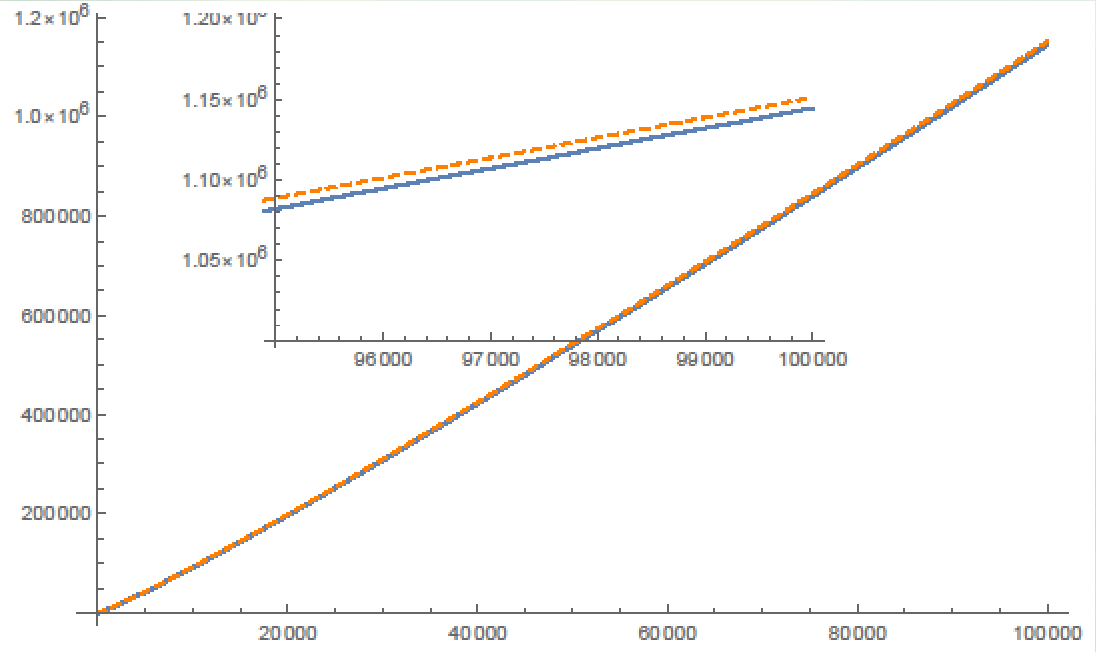
Numerics for $f(x) = x^2 + 1$

$$L_f(N) := \mathrm{LCM}(f(1), f(2), \ldots, f(N))$$

$$\log L_f(N) = N \log N + B_f\, N \ + \ o(N) \quad B_f \approx -0.066275634$$

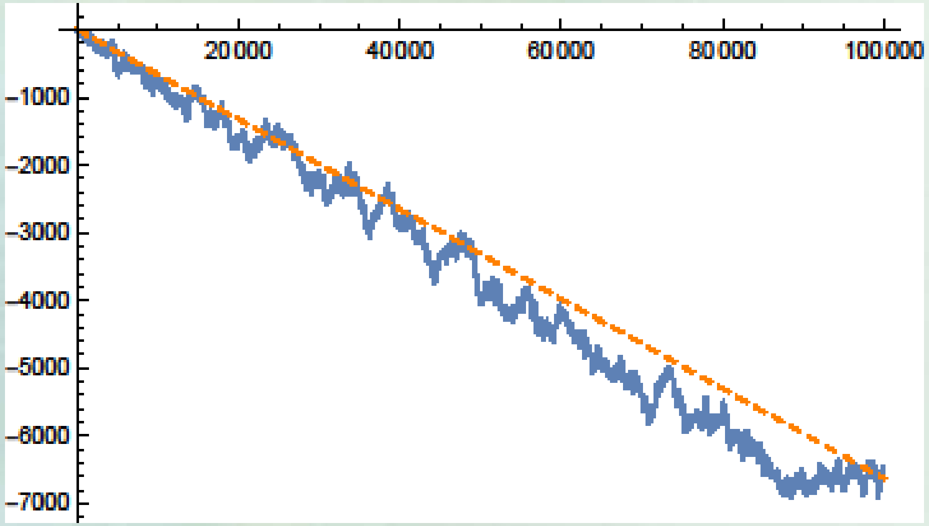


$\log L_f(N) - N\log N - B_f N$, $90{,}000 \leq N \leq 100{,}000$



$\log L_f(N)$ (solid) ▬▬ vs. $N \log N$ ----, N<100,000

Inset: 95000<N<100000

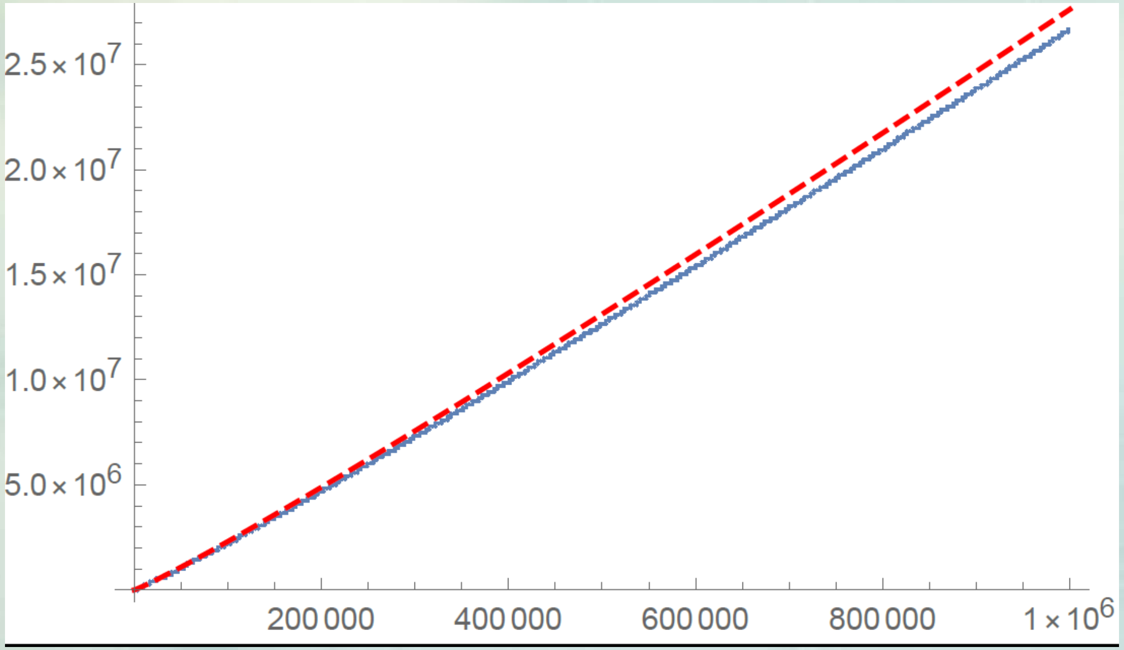


$\log L_f(N) - N\log N$ ▬▬ vs. $B_f N$ (----)

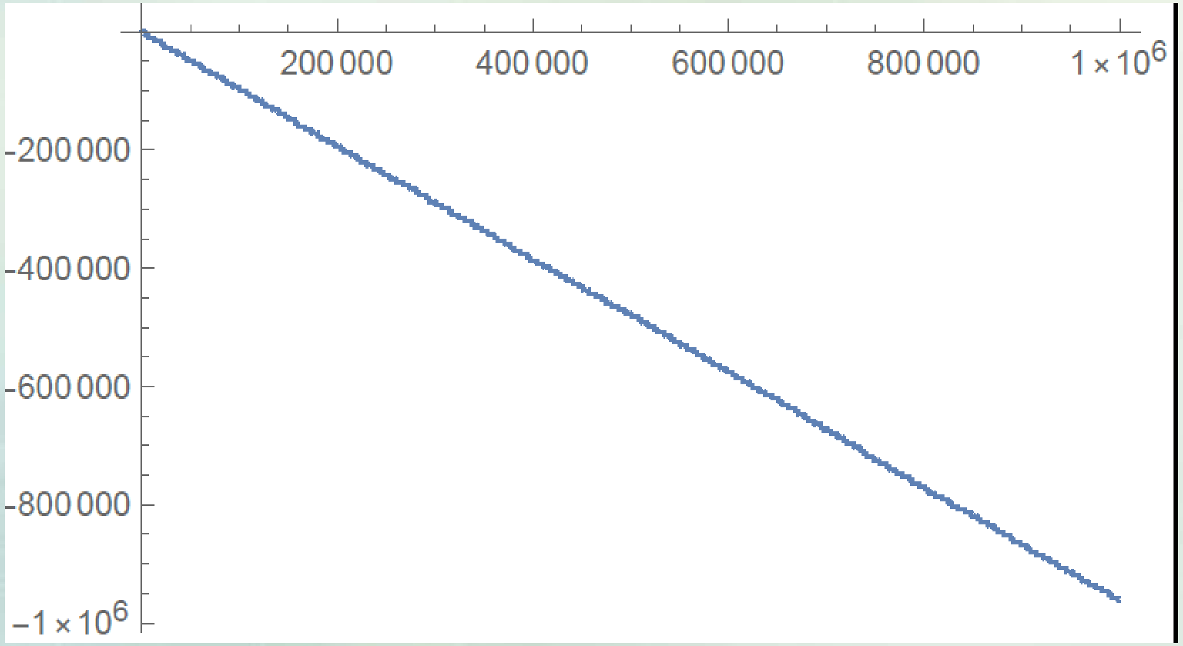
for N $\leq$ 100,000

Numerics for $f(x) = x^3 + 2$

$f(x) = x^3 + 2$ $\qquad L_f(N) := \mathrm{LCM}(f(1), f(2), \ldots, f(N))$

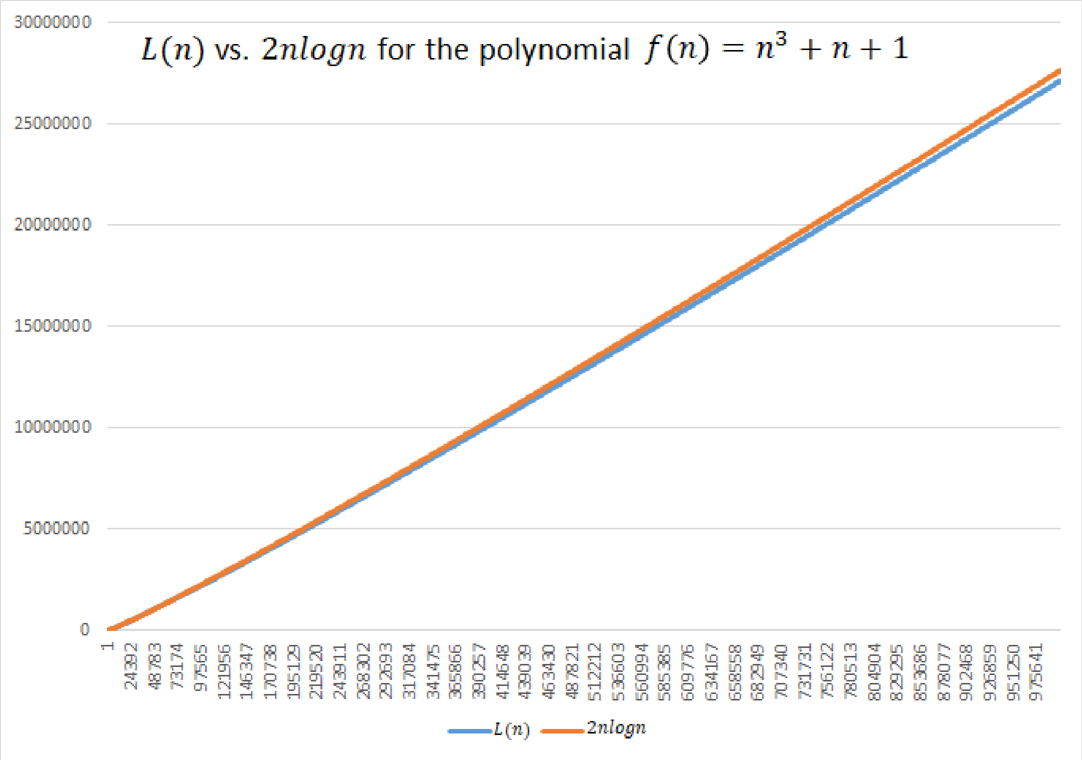


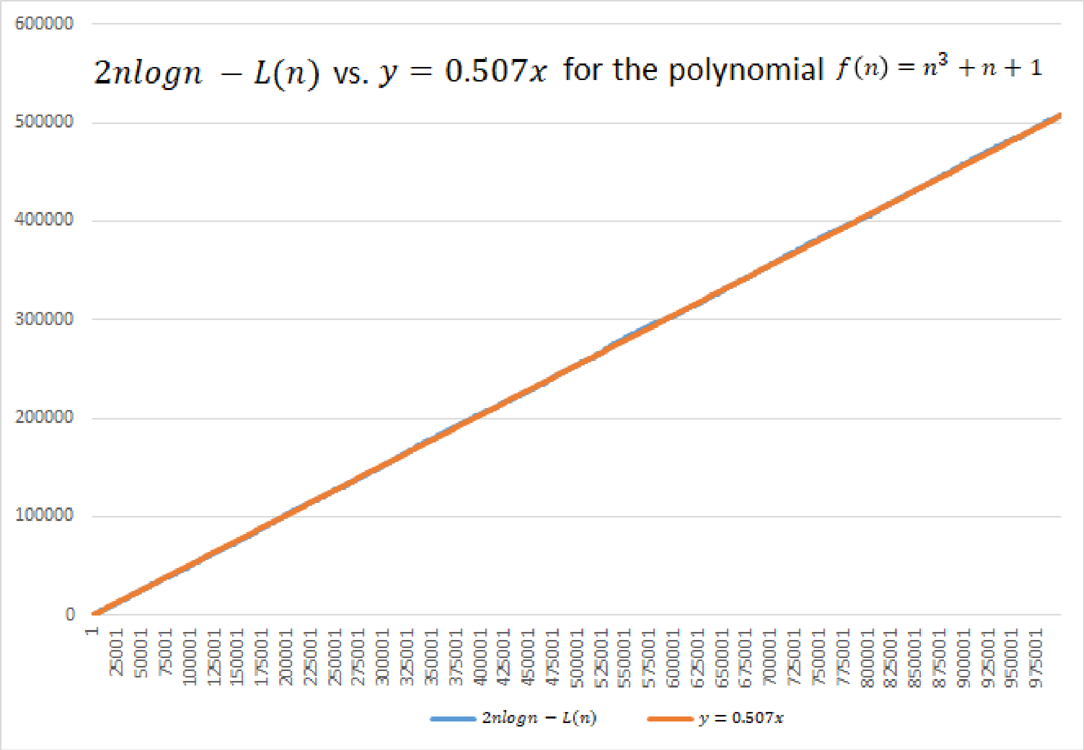
$\log L_f(N)$ ━━ $\quad 2N \log N$ - - - - -
$N \le 1{,}000{,}000$



$\log L_f(N) - 2N \log N, \quad N < 1{,}000{,}000$

Numerics for $f(x) = x^3 + x + 1$





$\log L_f(N)$ ▬ $2N \log N$ -----

$N \leq 1{,}000{,}000$

$2N \log N - \log L_f(N), \quad N < 1{,}000{,}000$

Reduction to small roots of congruences

Reduction to showing that modulo most big primes, $f(x)$ does not have **more** than one **small** root mod p

$$S_f(N) := \#\{p > N : \exists\, m \neq n \leq N : f(m) = 0 \bmod p \quad \text{and} \quad f(n) = 0 \bmod p\}$$

- Only need to check $p \ll N^{d-1}$

Cilleruelo:

$$\log L_f(N) = (d-1)N\log N - O(S_f(N)\log N) + o(N\log N)$$

→ **Upper bound**: For any irreducible f, $\log L_f(N) \ll N\log N$

Therefore

$$\log L_f(N) \sim (d-1)N\log N \iff S_f(N) = o(N)$$

Easy:

- $S_f(N) \ll N$
- For d=2, $S_f(N) = 0$

For $d = 2,\ S_f(N) = 0$

$$S_f(N) := \#\{p \gg N : \exists\, m \neq n \leq N : f(m) = 0 \bmod p \quad \text{and} \quad f(n) = 0 \bmod p\}$$

= primes $p \gg N$ s.t. $f(x)$ does not have more than one **small** root mod p

Check:

$$p \mid f(m) \quad \text{and} \quad p \mid f(n) \Rightarrow \mathrm{p} \mid f(m) - f(n)$$

$$f(x) = x^2 + 1 \quad \Rightarrow \quad \text{need} \quad p \mid f(m) - f(n) = (m^2+1) - (n^2+1) = (m-n)(m+n)$$

$$\Rightarrow p \mid m-n \quad or \quad p \mid m+n.$$

$$\text{if} \quad m < n \leq N \quad \text{and} \quad p \geq 2N \quad \text{this is impossible}$$

Cilleruelo (2011) : If f is **irreducible** and $\deg f = 2$, then $\log L_f(N) \sim N \log N$

An upper bound $S_f(N) \ll N$

Cilleruelo: $\log L_f(N) = (d-1)N\log N - O(S_f(N)\log N) + o(N\log N)$

$$S_f(N) := \#\{p \gg N : \exists\, m \neq n \leq N : f(m) = 0 \bmod p \quad \text{and} \quad f(n) = 0 \bmod p\}$$

$$S_f(N) \leq \sum_{p>N} \#\{n \leq N : p \mid f(n)\} = \sum_{n\leq N} \#\underbrace{\{p > N : p \mid f(n)\}}_{\leq d} \leq \sum_{n\leq N} d = dN$$

Want: $S_f(N) = o(N)$??

Random polynomials (ZR & Sa'ar Zehavi 2019)

There is no irreducible of degree >2 where the conjecture is known. So explore "typical" such polynomials.

Fix $f_0 \in \boldsymbol{Z}[x]$ monic of degree $d \geq 2$, and let $f_a(x) = f_0(x) - a$, with $a \in \boldsymbol{Z}$.

Fact: these are generically irreducible: the number of $|a| \leq T$ for which $f_0(x) - a$ is reducible is $O(\sqrt{T})$.

$$L(a;N) := \log \mathrm{LCM}(f_0(1)-a, f_0(2)-a, \ldots, f_0(N)-a)$$

Theorem: For almost all $|a| \leq T$

$$\log L(a;N) \sim (d-1) N \log N, \qquad \forall N \ \text{ s.t. } T^{1/(d-1)} < N < \frac{T}{\log T}$$

Random pols

We show that for almost all $|a| \leq T$, with $N \log N < T < N^{d-1}$

$$\log L(a;N) \sim (d-1)N \log N + O(S(a;N) \log N)$$

$$S(a;N) := \#\{ p \gg N : \exists\, m \neq n \leq N : f_0(m) - a = 0 \bmod p \quad \text{and} \quad f_0(n) - a = 0 \bmod p \}$$

Then show that for almost all $|a| \leq T, \;\; S(a;N) = o(N)$ by bounding expected value

$$\frac{1}{2T+1} \sum_{|a| \leq T} S(a;N) \ll \frac{N}{\log \log N}$$

A function field analogue

Let $\mathbb{F}_q$ the field of $q = p^r$ elements. Let $f(x) \in \mathbb{F}_q[t][x]$, irreducible over $\mathbb{F}_q(t)$.

For $\nu \gg 1$, set $N := q^\nu$. We define

$$L_f(N) := \text{lcm}\{ f\left(n(t)\right) : n(t) \in \mathbb{F}_q[t] \ \text{ monic}, \qquad \deg n \leq \nu \}$$

The condition $\deg n \leq \nu$ is equivalent to $\left|\left|n\right|\right| \leq N$. The condition $n(t)$ **monic** is analogous to the condition $n \geq 1$. So we have an analog quantity to

$$L_f(N) \coloneqq \text{lcm}\{ f(n) : n \in \boldsymbol{Z}, 1 \leq n \leq N\}$$

Theorem: Fix $q = 1 \bmod 3$. Let $f(x) = x^3 - a \in \mathbb{F}_q[t][x]$ with $a(t) \in \mathbb{F}_q[t]$ which is not a perfect cube in $\mathbb{F}_q[t]$. Then f is irreducible, and as $\nu = \log_q N \to \infty$,

$$\deg L_f(N) = 2N \log_q N + O(N).$$

Thank you for your attention!