Riv. Mat. Univ. Parma, Vol. **12** (2021), 143-150

James Maynard and Ze'ev Rudnick

A lower bound on the least common multiple of polynomial sequences

Abstract. For an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 2$, Cilleruelo conjectured that the least common multiple of the values of the polynomial at the first N integers satisfies $\log \operatorname{lcm}(f(1), \ldots, f(N)) \sim (d-1) N \log N$ as $N \to \infty$. This is only known for degree $d = 2$. We give a lower bound for all degrees $d \geq 2$ which is consistent with the conjecture: $\log \operatorname{lcm}(f(1), \ldots, f(N)) \gg N \log N$.

Keywords. Prime factor, polynomial, Chebotarev density Theorem.

Mathematics Subject Classification: 11N32.

1 - The LCM problem

For a polynomial $f \in \mathbb{Z}[X]$ with integer coefficients, set

$$L_f(N) := \operatorname{lcm}\{f(n) : n = 1, \ldots, N\}.$$

The goal is to understand the asymptotic growth of $\log L_f(N)$ as $N \to \infty$.

It is a well known and elementary fact that the least common multiple of all integers $1, 2, \ldots, N$ is exactly given by

$$\log \operatorname{lcm}\{1, 2, \ldots, N\} = \psi(N) := \sum_{n \leq N} \Lambda(n)$$

with $\Lambda(n)$ being the von Mangoldt function, and hence by the Prime Number Theorem,

$$\log \operatorname{lcm}\{1, 2, \ldots, N\} \sim N.$$

Received: October 28, 2019; accepted in revised form: March 19, 2020.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n^o 786758).

In the linear case $\deg f = 1$, we still have $\log L_f(N) \sim c_f N$ from the Prime Number Theorem in arithmetic progressions [**1**]. A similar growth occurs for products of linear polynomials [**6**].

However, in the case of irreducible polynomials of higher degree, Cilleruelo [**3**] conjectured that the growth is faster than linear, precisely:

Conjecture 1.1. *If f is an irreducible polynomial with $\deg f \geq 2$, then*

$$\log L_f(N) \sim (\deg f - 1) N \log N, \quad N \to \infty.$$

Cilleruelo proved Conjecture 1.1 for quadratic polynomials. No other case of Conjecture 1.1 is known to date.

Remark. *An examination of Cilleruelo's argument shows that for any irreducible f of degree $d \geq 3$, we have an upper bound*

$$\log L_f(N) \lesssim (d-1) N \log N.$$

Here $f \lesssim g$ means that $|f(x)| \leq (1+o(1))g(x)$.

In this note, we give a lower bound of the right order of magnitude:

Theorem 1.2. *Let $f \in \mathbb{Z}[x]$ be irreducible, of degree $d \geq 2$. Then*

$$\log L_f(N) \gg N \log N.$$

Remark. *The argument gives that $\log L_f(N) \gtrsim \frac{1}{d} N \log N$.*

Corollary 1.3. *Suppose $f \in \mathbb{Z}[x]$ has an irreducible factor of degree ≥ 2, i.e. $f(x)$ is not a product of linear polynomials (over $\mathbb{Q}$). Then*

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

This is because $\max(\operatorname{lcm}\{a_n\}, \operatorname{lcm}\{b_m\}) \leq \operatorname{lcm}\{a_n b_n\} \leq \operatorname{lcm}\{a_n\} \cdot \operatorname{lcm}\{b_m\}$.

Prior to this note, the only available bound was of size $\gg N$: Hong *et al* [**5**] show that $\log L_f(N) \gg N$ for any polynomial with *non-negative* integer coefficients.

2 - Proof of Theorem 1.2

Let $P^+(n)$ denote the largest prime factor of n. We will need a result on the greatest prime factor $P^+(f(n))$ of $f(n)$ ("Chebyshev's problem"). This is a well-studied subject, and we need a relatively simple bound, which we state here and explain in § 3:

Theorem 2.1. *Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree $d \geq 2$. Then*

$$P^+(f(n)) > n$$

for a positive proportion of integers n.

Remark. *In fact one can show $P^+(f(n)) > n$ for a proportion at least $1 - \frac{1}{d}$ of integers n.*

A result of this form goes back to T. Nagell in 1921 [**7**], though he did not state this with positive density, but instead with a better bound of $n(\log n)^a$ for all $a < 1$. Once one gets that $P^+(f(n)) > n$ holds on a set of positive density, one automatically obtains a better bound of $P^+(f(n)) \gg n \log n$, again in a set of positive density, see § 3. A form of Theorem 2.1 was given by Cassels [**2**] in 1960. The problem was studied by Erdős [**4**] in 1952, and in 1990 Tenenbaum [**8**] showed that $P^+(f(n)) > n \exp((\log n)^a)$ infinitely often for all $a < 2 - \log 4$.

Alongside Theorem 2.1, we need the following simple lemma. Let

$$\mathcal{N} := \Big\{ n \in \Big[\frac{N}{\log N}, N\Big] : P^+(f(n)) > n \Big\}.$$

Lemma 2.2. *Given a prime p, and for N sufficiently large in terms of f, the number of $m \in \mathcal{N}$ with $P^+(f(m)) = p$ is at most d.*

Proof. If $P^+(f(m)) = p$ then we must have

$$f(m) \equiv 0 \pmod{p}.$$

If $m \in \mathcal{N}$ and $P^+(f(m)) = p$ we must also have that $N/\log N \leq m < p$. Since $p > N/\log N$ and N is sufficiently large in terms of f, we see that f is a non-zero polynomial modulo p. Therefore f has at most d roots modulo p, and all choices of m must be congruent to one of these roots. Since we only consider $0 < m < p$, there is at most one choice of $m \equiv a \pmod{p}$ for each root a modulo p, and so at most d choices of m. □

2.1 - *Proof of Theorem 1.2*

Given Theorem 2.1, we proceed as follows. The result is trivial for bounded N, so we may assume that N is sufficiently large in terms of f. By Theorem 2.1, there is an absolute constant $c > 0$ such that $P^+(f(n)) > n$ for $\gtrsim cN$ integers in $[1, N]$, and so certainly $\#\mathcal{N} \gtrsim cN$. Let

$$\mathcal{P} := \{P^+(f(n)) : n \in \mathcal{N}\}$$

be the set of largest prime factors occurring. Then, by Lemma 2.2, we have that

$$cN \lesssim \#\mathcal{N} = \sum_p \#\{n \in \mathcal{N} : P^+(f(n)) = p\} \le d\#\mathcal{P},$$

and so

$$\#\mathcal{P} \gtrsim \frac{cN}{d}.$$

Moreover, by definition of $\mathcal{N}$, if $p \in \mathcal{P}$ then $p > N/\log N$ and $p|f(n)$ for some $n \le N$. Therefore we have that

$$\begin{aligned}\log \operatorname{lcm}(f(1), \dots, f(N)) &\ge \sum_{p \in \mathcal{P}} \log p \ge \#\mathcal{P} \log \frac{N}{\log N} \\ &\gtrsim \frac{cN}{d} \log N,\end{aligned}$$

as claimed. □

3 - Proof of Theorem 2.1

We begin by recording a simple bound on the number of times a prime p can divide values of f. Let $\alpha_p(N)$ be the exponents in the prime factorization

$$\prod_{n=1}^N |f(n)| = \prod_p p^{\alpha_p(N)}.$$

We then have the following result.

Lemma 3.1. *Let $\rho_f(m)$ denote the number of roots of f modulo m. Assume that f has no rational zeros. Let p be a prime, $p \le N$.*

Then if $p \nmid \operatorname{disc} f$, we have

$$\alpha_p(N) = N\frac{\rho_f(p)}{p-1} + O\Big(\frac{\log N}{\log p}\Big) \tag{1}$$

and if $p \mid \operatorname{disc} f$, we have

$$\alpha_p(N) \ll \frac{N}{p}.$$

Proof. Since f has no rational zeros, $\prod_{n=1}^N f(n) \ne 0$ and so $\alpha_p(N)$ is well defined. By definition,

$$\alpha_p(N) = \sum_{n \le N} \sum_{k \ge 1} \mathbf{1}(p^k \mid f(n)) = \sum_{1 \le k \lesssim \frac{d \log N}{\log p}} \#\{n \le N : f(n) = 0 \bmod p^k\}.$$

To count the number $\#\{n \le N : f(n) = 0 \bmod p^k\}$, divide the interval $[1, N]$ into $\lfloor N/p^k \rfloor$ consecutive intervals of length p^k, and a remaining interval. On each such interval of length p^k, the number of solutions of $f(n) = p^k$ is the total number $\rho_f(p^k)$ of solutions of this congruence. On the remaining interval, the number of solutions is not greater than that. Hence

$$\alpha_p(N) = \sum_{1 \le k \lesssim \frac{d \log N}{\log p}} \rho_f(p^k) \left(\left\lfloor \frac{N}{p^k} \right\rfloor + O(1) \right).$$

By Hensel's lemma, $\rho_f(p^k) = \rho_f(p)$ for $p \nmid \operatorname{disc} f$. Hence for $p \nmid \operatorname{disc} f$

$$\alpha_p(N) = \sum_{1 \le k \lesssim \frac{d \log N}{\log p}} \rho_f(p) \left(\left\lfloor \frac{N}{p^k} \right\rfloor + O(1) \right) = \rho_f(p) \left(\frac{N}{p-1} + O\left(\frac{\log N}{\log p} \right) \right).$$

For primes $p \mid \operatorname{disc} f$ dividing the discriminant of f, a more detailed examination gives the bound [**7**, Théorème II]

$$\rho_f(p^k) \le d(\operatorname{disc} f)^2 = O(1)$$

which gives for $p \mid \operatorname{disc} f$

$$\alpha_p(N) \ll_f \sum_{1 \le k \lesssim \frac{d \log N}{\log p}} \left(\left\lfloor \frac{N}{p^k} \right\rfloor + O(1) \right) \ll \frac{N}{p},$$

as claimed. □

Proof. Let $N_- := N/\log N$, and define the exceptional set $\mathcal{E}(N) \subseteq (N_-, N]$ by

$$\mathcal{E}(N) := \{N_- < n \le N : P^+(f(n)) \le n\}.$$

Let

$$Q(N) := \prod_{n \in \mathcal{E}(N)} |f(n)|.$$

We compute $\log Q(N)$ in two ways:

Using $\log |f(n)| \sim d \log n$ as $n \to \infty$, we have

$$\log Q(N) = \sum_{n \in \mathcal{E}(N)} \log |f(n)| \sim \sum_{n \in \mathcal{E}(N)} d \log n.$$

Since $\log n \sim \log N$ for $n \in \mathcal{E}(N) \subseteq [N_-, N]$, we have

$$\sum_{n \in \mathcal{E}(N)} d \log n \sim d \log N \# \mathcal{E}(N)$$

so that

$$\log Q(N) \sim d \log N \# \mathcal{E}(N). \tag{2}$$

On the other hand, write the prime power decomposition of $Q(N)$ as

$$Q(N) = \prod_{n \in \mathcal{E}(N)} |f(n)| = \prod_p p^{\gamma_p(N)}.$$

Since $P^+(f(n)) \le n \le N$ for all $n \in \mathcal{E}(N)$, only primes $p \le N$ appear in the product. Thus

$$\log Q(N) = \sum_{p \le N} \gamma_p(N) \log p.$$

We also have $\gamma_p(N) \le \alpha_p(N)$ where $\prod_{n=1}^N |f(n)| = \prod_p p^{\alpha_p(N)}$. Thus

$$\log Q(N) \le \sum_{p \le N} \alpha_p(N) \log p.$$

Therefore, by Lemma 3.1,

$$\begin{aligned} \log Q(N) &\le \sum_{p \le N} \alpha_p(N) \log p \\ &\le \sum_{p \le N} \left(N \frac{\rho_f(p)}{p-1} + O\left(\frac{\log N}{\log p} \right) \right) \log p + O\left(\sum_{p | \operatorname{disc} f} \frac{N \log p}{p} \right) \\ &= N \sum_{p \le N} \frac{\rho_f(p) \log p}{p-1} + O\Big(\pi(N) \log N \Big) + O(N). \end{aligned}$$

Now for f irreducible it follows from the Chebotarev density theorem (or earlier work of Kronecker or Frobenius) that (see [**7**, equation (4)]):

$$\sum_{p \le N} \frac{\rho_f(p) \log p}{p-1} = \log N + O(1),$$

hence

$$\log Q(N) \le N \Big(\log N + O(1) \Big) + O(N) \sim N \log N.$$

Comparing with (2) gives

$$d \log N \# \mathcal{E}(N) \lesssim \log Q(N) \lesssim N \log N$$

and hence we obtain

$$\# \mathcal{E}(N) \lesssim \frac{1}{d} N.$$

Therefore

$$\#\{n \in [1,N] : P^+(f(n)) < n\} \le N_- + \#\mathcal{E}(N) \lesssim N_- + \frac{1}{d}N \lesssim \frac{1}{d}N,$$

that is the proportion of elements of $[1,N]$ with $P^+(f(n)) < n$ is at most $1/d$.□

We owe to Andrew Granville the following observation: Theorem 2.1 can be boot-strapped to give a slightly better result:

Corollary 3.2. *Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree $d \ge 2$. Then for any $\delta < 1/d^2$,*

$$P^+(f(n)) > \delta n \log n$$

for a positive proportion of the integers.

Proof. Let $\delta > 0$ be fixed, and let

$$\mathcal{S} := \Big\{n \in \Big[\frac{N}{\log N}, N\Big] : P^+(f(n)) < \delta n \log n\}.$$

Assume by contradiction that $\mathcal{S}$ has full density, that is $\#\mathcal{S} \sim N$ as $N \to \infty$. As before, let

$$\mathcal{N} := \{\frac{N}{\log N} < n \le N : P^+(f(n)) > n\}.$$

We saw that $\#\mathcal{N} \gtrsim \frac{1}{d}N$. Since $\#\mathcal{S} \sim N$ by assumption, we see that $\#\mathcal{N} \cap \mathcal{S} \gtrsim \frac{1}{d}N$. Let

$$\mathcal{P}_{\mathcal{S}} := \{P^+(f(n)) : n \in \mathcal{S} \cap \mathcal{N}\}$$

be the set of largest prime divisors arising from $n \in \mathcal{N} \cap \mathcal{S}$. Then we saw in Lemma 2.2 that each prime $p \in \mathcal{P}_N$ can occur at most d times as some $P^+(f(m))$ for $m \in \mathcal{N}$, and so

$$\#\mathcal{P}_{\mathcal{S}} \ge \frac{1}{d}\#\mathcal{N} \cap \mathcal{S} \gtrsim \frac{1}{d^2}N.$$

On the other hand, since $P^+(f(n)) < \delta n \log n$ for $n \in \mathcal{S} \cap \mathcal{N}$, we must have $\mathcal{P}_{\mathcal{S}} \subseteq [1, \delta N \log N]$. Therefore

$$\#\mathcal{P}_{\mathcal{S}} \le \pi(\delta N \log N) \sim \delta N$$

by the Prime Number Theorem. Thus

$$\frac{1}{d^2}N \lesssim \#\mathcal{P}_{\mathcal{S}} \lesssim \delta N$$

which is a contradiction if $\delta < 1/d^2$. □

Acknowledgments. We thank the referee for their careful reading of our paper.

References

[**1**] P. Bateman, J. Kalb and A. Stenger, *A Limit Involving Least Common Multiples: 10797*, Am. Math. Mon. **109** (2002), no. 4, 393–394.

[**2**] J. W. S. Cassels, *Footnote to a note of Davenport and Heilbronn*, J. London Math. Soc. **36** (1961), 177–184.

[**3**] J. Cilleruelo, *The least common multiple of a quadratic sequence*, Compos. Math. **147** (2011), no. 4, 1129–1150.

[**4**] P. Erdős, *On the greatest prime factor of* $\prod_{k=1}^{x} f(k)$, J. London Math. Soc. **27** (1952), 379–384.

[**5**] S. Hong, Y. Luo, G. Qian and C. Wang, *Uniform lower bound for the least common multiple of a polynomial sequence*, C. R. Math. Acad. Sci. Paris **351** (2013), no. 21-22, 781–785.

[**6**] S. Hong, G. Qian and Q. Tan, *The least common multiple of sequence of product of linear polynomials*, Acta Math. Hungar. **135** (2012), no.1-2, 160–167.

[**7**] T. Nagel, *Généralization d'un théorème de Tchebycheff*, J. Math. Pures Appl. **4** (1921), 343–356.

[**8**] G. Tenenbaum, *Sur une question d'Erdős et Schinzel, II*, Invent. Math. **99** (1990), 215–224.

James Maynard
Mathematical Institute
Radcliffe observatory quarter
Woodstock Road, Oxford OX2 6GG, England
e-mail: james.alexander.maynard@gmail.com

Ze'ev Rudnick
Raymond and Beverly Sackler School of Mathematical Sciences
Tel Aviv University
Tel Aviv 69978, Israel
e-mail: rudnick@tauex.tau.ac.il