ASYMPTOTIC IMPROVEMENTS OF LOWER BOUNDS FOR THE LEAST COMMON MULTIPLES OF ARITHMETIC PROGRESSIONS

DANIEL M. KANE AND SCOTT DUKE KOMINERS

ABSTRACT. For relatively prime positive integers u_0 and r, we consider the least common multiple $L_n := \mathrm{lcm}(u_0, u_1, \ldots, u_n)$ of the finite arithmetic progression $\{u_k := u_0 + kr\}_{k=0}^{n}$. We derive new lower bounds on L_n which improve upon those obtained previously when either u_0 or n is large. When r is prime, our best bound is sharp up to a factor of $n + 1$ for u_0 properly chosen, and is also nearly sharp as $n \to \infty$.

1. Introduction

The search for effective bounds on the least common multiples of arithmetic progressions began with the work of Hanson [Han72] and Nair [Nai82], who respectively found upper and lower bounds for $\mathrm{lcm}(1, \ldots, n)$. Decades later, Bateman, Kalb, and Stenger [BKS02] and Farhi [Far05] respectively obtained asymptotics and nontrivial lower bounds for the least common multiples of general arithmetic progressions. The bounds of Farhi [Far05] were then successively improved by Hong and Feng [HF06], Hong and Yang [HY08], Hong and the second author [HK10], and Tan and Hong [TH10]. Farhi and the first author [FK09] also obtained some related results regarding $\mathrm{lcm}(u_0 + 1, \ldots, u_0 + n)$, which have recently been generalized to general arithmetic progressions by Hong and Qian [HQ10].

In this article, we study finite arithmetic progressions $\{u_k := u_0 + kr\}_{k=0}^{n}$ with $u_0, r \geq 1$ integers satisfying $(u_0, r) = 1$. Throughout, we let $n \geq 0$ be a nonnegative integer and define

$$L_n := \mathrm{lcm}(u_0, \ldots, u_n)$$

to be the least common multiple of the sequence $\{u_0, \ldots, u_n\}$.

We derive new lower bounds on L_n which improve upon those obtained previously when either u_0 or n is large. After introducing relevant notation and preliminary results in Section 2, we develop and prove our bounds in Section 3. Then, in Section 4, we show that our best bound is sharp up to a factor of $n+1$ for u_0 properly chosen and r prime. We study asymptotics for large n in Section 5, showing that our best bound is nearly sharp as $n \to \infty$ when r is prime. We conclude in Section 6.

As we discuss in Section 6, our approach extends the methods of Hong and Feng [HF06] and the subsequent work ([HY08, HK10, TH10]), pushing these methods nearly to their limits. The asymptotic estimates we obtain in Section 5.2 suggest that still better bounds may be possible, but these bounds will likely require new techniques.

2000 *Mathematics Subject Classification.* 11A05 (primary).

Key words and phrases. Least common multiple, arithmetic progression.

2. Preliminaries

Following Hong and Feng [HF06] and the subsequent work, we denote, for each integer $0 \le k \le n$,

$$C_{n,k} := \frac{u_k \cdots u_n}{(n-k)!}, \quad L_{n,k} := \operatorname{lcm}(u_k, \ldots, u_n).$$

From the latter definition, we have that $L_n = L_{n,0}$.

We now note two preliminary lemmata which we will use in the sequel. First, we state the following lemma which first appeared in [Far05] and has been reproven in several sources.

Lemma 1 ([Far05],[Far07],[HF06])**.** *For any integer $n \ge 1$, $C_{n,0} \mid L_n$.*

From Lemma 1, we see immediately that, for all k with $0 \le k \le n$,

$$L_{n,k} = A_{n,k} \frac{u_k \cdots u_n}{(n-k)!} = A_{n,k} \cdot C_{n,k}$$

for an integer $A_{n,k} \ge 1$.

Now, we introduce an intuitive lemma regarding the highest power of an integer dividing a factorial.

Lemma 2. *If $s \ge 0$ and $m \ge 0$ are positive integers, then $s^a \mid m!$ for some integer*

$$a \ge \frac{m}{s-1} - \log_s(m+1).$$

The proof of Lemma 2 is a simple generalization of the well-known form of Lemma 2 in the case that s is prime. Since Lemma 2 does not appear to be easily accessible in the literature, we include its proof in Appendix A.

3. The Basic Bound

Theorem 3. *Given u_0, r, and n as above, and letting k be an integer with $0 \le k \le n$, we have that*

$$L_n \ge \frac{u_k \cdots u_n}{(n-k)!} \prod_{p \mid r} \left(\frac{p^{(n-k)/(p-1)}}{n-k+1} \right), \tag{1}$$

where the product runs over primes p dividing r.

Proof. We begin by noting that

$$L_n = \operatorname{lcm}(u_0, \ldots, u_n) \ge \operatorname{lcm}(u_k, \ldots, u_n) = L_{n,k}.$$

We recall that $L_{n,k} = C_{n,k} A_{n,k}$, where

$$C_{n,k} := \frac{u_k \cdots u_n}{(n-k)!}$$

and $A_{n,k}$ is an integer. We notice that any prime p dividing r does not divide $u_k \cdots u_n$. Therefore, since $L_{n,k}$ is an integer, any power of p dividing $(n-k)!$ must also divide $A_{n,k}$. By Lemma 2, we know that $(n-k)!$ is divisible by p^{a_p}, with

$$a_p \ge \frac{n-k}{p-1} - \log_p(n-k+1).$$

Hence, we have

$$A_{n,k} \geq \prod_{p|r} p^{a_p} \geq \prod_{p|r} \left(\frac{p^{(n-k)/(p-1)}}{n-k+1} \right).$$

It then follows that

$$L_n \geq L_{n,k} = C_{n,k} A_{n,k} \geq \frac{u_k \cdots u_n}{(n-k)!} \prod_{p|r} \left(\frac{p^{(n-k)/(p-1)}}{n-k+1} \right). \qquad \square$$

We note that the term

$$\frac{p^{(n-k)/(p-1)}}{n-k+1}$$

which arises in the product term of (1) is the quotient of an exponential by a polynomial. In particular, it grows quickly and is at least 1 as long as $n-k \geq p-1$.

Additionally, we note a second bound which follows by an argument similar to that used to prove Theorem 3.

Theorem 4. *Given u_0, r, and n as above and letting k be an integer with $0 \leq k \leq n$, we have that*

$$L_n \geq \frac{u_k \cdots u_n}{(n-k)!} \left(\frac{r^{(n-k)/(r-1)}}{n-k+1} \right). \tag{2}$$

The bounds of Theorems 3 and 4 agree when r is prime. Also, we may rearrange the terms on the right-hand side of (2) to obtain the following equivalent form of the bound (2) of Theorem 4.

Corollary 5. *Given u_0, r, and n as above and letting k be an integer with $0 \leq k \leq n$, we have that*

$$L_n \geq r^{\frac{(n-k)r}{r-1}} \binom{\left(\frac{u_{k-1}}{r}\right) + (n-k+1)}{n-k+1}. \tag{3}$$

We now determine the value of k which yields the best bound in Corollary 5. It is clear that increasing k in (3) increases the right-hand term of (3) by a factor of

$$\frac{n-k+1}{u_k r^{\frac{1}{r-1}}}.$$

Since this factor is decreasing in k, the optimal bound (3) is achieved when

$$k = k^* := \max\left\{0, \left\lceil \frac{n+1-u_0 r^{1/(r-1)}}{r^{r/(r-1)}+1} \right\rceil \right\}.$$

3.1. **Remarks.** The best previous bound on L_n is given by the following result of Tan and Hong [TH10].

Theorem 6 ([TH10])**.** *Let $a, \ell \geq 2$ by given integers. Then for any integers $\alpha \geq a$ and $r \geq \max(a, \ell-1)$ and $n \geq \ell\alpha r$, we have that $L_n \geq u_0 r^{(\ell-1)\alpha+a-\ell}(r+1)^n$.*

Note that for $n \geq r^2(r+1)$ the bound of Theorem 6 is maximized when $a = r$ and $\ell = r+1$ and $\alpha = \left\lfloor \frac{n}{r(r+1)} \right\rfloor$, yielding

$$L_n \geq u_0 r^{r\left\lfloor \frac{n}{r(r+1)} \right\rfloor - 1}(r+1)^n,$$

which is asymptotically weaker than our bound as $n \to \infty$.

The proof of Theorem 6 comes from bounding $A_{n,k}$ below by

$$r^{r\left\lfloor \frac{n}{r(r+1)} \right\rfloor - 1}$$

in the case that

$$k = \max\left\{0, \left\lfloor \frac{n-u_0}{r+1} \right\rfloor + 1\right\} \approx \frac{n}{r+1},$$

and then bounding $C_{n,k}$ below by $u_0(r+1)^n$. We improve upon Theorem 6 in several ways. First, our lower bound on $A_{n,k}$ is much better, provided that n is sufficiently large. Second, we pick the exact value of k which optimizes our lower bound. Lastly, we keep $C_{n,k}$ in its native form, rather than replacing it by a smaller value; this improvement is particularly helpful when u_0 is large.

4. Bounds for Large u_0

When u_0 is large, we have $k^* = 0$ and therefore get the best bound from Corollary 5 by setting $k = 0$ in (3). This indicates that the following corollary of Theorem 3 is sharpest for large u_0.

Corollary 7. *Given u_0, r, and n as above, we have that*

$$L_n \geq r^{\frac{nr}{r-1}} \binom{\frac{u_0}{r} + n}{n+1}. \tag{4}$$

4.1. **Remarks.** If u_0 is divisible by the part of $\operatorname{lcm}(1, \ldots, n)$ relatively prime to r, then $A_{n,0}$ is just the largest divisor of $n!$ divisible only by primes dividing r. In particular, if r is also prime, then the bound given in (4) is sharp up to the error in Lemma 2. On the other hand, it is the case that for p prime, the largest a so that $p^a \mid n!$ is at most $n/(p-1)$. Therefore, for appropriately chosen u_0, and r prime, the bound (4) of Corollary 7 is sharp to within a factor of $n+1$.

5. Asymptotics for Large n

We will now determine the asymptotics of the lower bound (3) of Corollary 5 when n is large relative to u_0 and r. We notice that for n large and k near its optimal value, k^*, the multiplicative change in (3) as k is increased or decreased by 1 is close to 1. Furthermore, if the binomial coefficient in (3) is interpolated using the Gamma function, this will hold even for fractional values of k. Hence, we will still get the optimal bound asymptotically if we use (3) with any k within $O(1)$ of k^*.

Now, we set

$$\tilde{k}^* := 1 + \frac{n}{r^{r/(r-1)} + 1} - \frac{u_0}{r(r^{-r/(r-1)} + 1)},$$

noting that $\tilde{k}^*$ is with $O(1)$ of k^* for all n. We set

$$\beta := r^{-r/(r-1)} = \frac{\left(\frac{u_{\tilde{k}^*-1}}{r}\right) + (n - \tilde{k}^* + 1)}{n - \tilde{k}^* + 1} - 1,$$

hence if we take $k = \tilde{k}^*$ in (3), the ratio of the terms in the binomial coefficient will equal $\beta + 1$. For ease of notation, we also denote

$$\mu := \left(\frac{u_{\tilde{k}^*-1}}{r}\right) + (n - \tilde{k}^* + 1) = \frac{u_n}{r},$$

so that the binomial coefficient in (3) with $k = \tilde{k}^*$ is

$$\binom{\mu}{\mu/(\beta+1)}. \tag{5}$$

By Stirling's formula, (5) is asymptotic to

$$\frac{1+\beta}{\sqrt{2\pi\mu\alpha}} \left((1+\beta)^{\frac{1}{1+\beta}} \left(\frac{1+\beta}{\beta} \right)^{\frac{\beta}{1+\beta}} \right)^{\mu}.$$

It follows that our lower bound is asymptotic to

$$r^{\frac{(n-\tilde{k}^*)r}{r-1}} \left(\frac{1+\beta}{\sqrt{2\pi\mu\beta}} \right) \left((1+\beta)^{\frac{1}{1+\beta}} \left(\frac{1+\beta}{\beta} \right)^{\frac{\beta}{1+\beta}} \right)^{\mu}. \tag{6}$$

The exponential part of (6) is

$$\left(r^{\frac{r}{(1+\beta)(r-1)}} (1+\beta)^{\frac{1}{1+\beta}} \left(\frac{1+\beta}{\beta} \right)^{\frac{\beta}{1+\beta}} \right)^{n}. \tag{7}$$

5.1. **True Asymptotics.** If we fix u_0 and r, it is actually possible to derive an asymptotic formula for $\log(L_n)$. This is acheived by noting that

$$\log(L_n) = \sum_{d \mid L_n} \Lambda(d),$$

where $\Lambda(d)$ is the Von Mangoldt function. By definition, $\Lambda(d)$ is zero unless d is a power of a prime. Furthermore, for d a power of a prime, $d \mid L_n$ if and only if $d \mid u_k$ for some k ($0 \le k \le n$). Therefore we have that

$$\log(L_n) = \sum_{\substack{d \mid u_k \\ \text{for some } 0 \le k \le n}} \Lambda(d). \tag{8}$$

Next, we observe that if n is sufficiently large, L_n will be divisible by all of the finitely many positive integers less than u_0 and congruent to u_0 modulo r. If this holds, the d in (8) will be exactly the d dividing some positive integer $U \le u_n$ with $U \equiv u_0 \bmod r$. Clearly the smallest positive integer congruent to u_0 modulo r and divisible by d is $d \cdot \ell_d$, where ℓ_d is the smallest positive representative of the conjugacy class of $\frac{u_0}{d}$ modulo r. Hence, we may break up the sum in (8) to obtain

$$\log(L_n) = \sum_{\substack{(\ell,r)=1 \\ 0<\ell<r}} \sum_{\substack{d < \frac{u_n}{\ell} \\ d \equiv \frac{u_0}{\ell} \bmod r}} \Lambda(d). \tag{9}$$

We recall that the inner sum in (9) is asymptotic to $\left(\frac{1}{\varphi(r)}\right)\left(\frac{u_n}{\ell}\right)$, where φ is the Euler totient function (see [IK04, p. 122, eq. (5.71)]). Therefore, we have that

$$\log(L_n) \sim \frac{u_n}{\phi(r)} \sum_{\substack{(\ell,r)=1 \\ 0<\ell<r}} \frac{1}{\ell}. \tag{10}$$

If we assume that r is prime, (10) reduces to

$$\log(L_n) \sim \frac{u_n}{r-1} H_{r-1}, \tag{11}$$

where H_{r-1} denotes the $(r-1)$-st harmonic number.

5.2. **Remarks.** We note that our proven asymptotic for $\log(L_n)$ has linear term

$$n\left(\frac{rH_{r-1}}{r-1}\right)=n\left(\log(r)+\gamma+O\left(\frac{\log(r)}{r}\right)\right),$$

where γ is the Euler-Mascheroni constant. The asymptotic lower bound (6) we prove has exponential term (7) with logarithm

$$n\left(\frac{r\log(r)}{(r-1)(\beta+1)}+\frac{\log(1+\beta)}{1+\beta}+\left(\frac{\beta}{1+\beta}\right)\log\left(\frac{1+\beta}{\beta}\right)\right)=n\left(\log(r)+O\left(\frac{\log(r)}{r}\right)\right),$$

as we have $\alpha = O\left(\frac{1}{r}\right)$. Thus, we see that our bound (3) of Corollary 5 is within a multiplicative factor of approximately $e^{\gamma n}$ of being asymptotically sharp.

6. Conclusion

Determining lower bounds on L_n is clearly equivalent to the problem of finding lower bounds for $A_{n,k}$. We have so far obtained these bounds by noting that, although $L_{n,k}$ is always an integer, $C_{n,k}$ need not be integral. In essence, this is the same strategy which has been applied in the work of Hong and Feng [HF06], Hong and Yang [HY08], Hong and the second author [HK10], and Tan and Hong [TH10]. Unfortunately, in this article, we have apparently pushed these techniques nearly to their limits. It is relatively easy to show that $C_{n,k}$ does not have in its denominator any prime factors which do not also divide r. Furthermore, we have accounted almost exactly for the contributions of these primes to the denominator of $C_{n,k}$. Hence, further progress towards bounding L_n should come from new techniques for bounding $A_{n,k}$.

Fortunately, there is hope that better bounds on $A_{n,k}$ can be obtained. The proof that $C_{n,k}$ divides $L_{n,k}$ considers the potential common divisors of the elements $\{u_k,\ldots,u_n\}$. On the other hand, unless u_k is chosen very carefully, not all of these common divisors actually appear. In particular, for $A_{n,k}$ to have no factors prime to r, it will need to be the case that the part of $n-k-m$ prime to r divides $u_k\cdots u_{k+m}$ for each m. For each such divisibility condition which fails, we gain extra factors for $A_{n,k}$. Furthermore, we know that such factors must exist since (as was shown in Section 5.2), for large n and prime r, our bound fails by a factor of roughly $e^{\gamma n}$.

Acknowledgements

While working on this paper, the first author was partly supported by NDSEG and NSF Graduate Research Fellowships, and the second author was partly supported by an NSF Graduate Research Fellowship. Both authors thank Noam D. Elkies and Benedict H. Gross for helpful comments and suggestions.

Appendix A. Proof of Lemma 2

We notice that $\left\lfloor\frac{m}{s}\right\rfloor$ of the integers $1,\ldots,m$ are divisible by s. More generally $\left\lfloor\frac{m}{s^i}\right\rfloor$ of these integers are divisible by s^i. Each such term provides us with a new factor of s dividing $m!$. Hence, if $a=\sum_{i=1}^{\infty}\left\lfloor\frac{m}{s^i}\right\rfloor$, then $s^a \mid m!$.

We now show that this a is at least $\frac{m}{s-1}-\log_s(m+1)$. First, it follows easily by induction upon m that $\sum_{i=1}^{\infty}\left\lfloor\frac{m}{s^i}\right\rfloor=\frac{m-d}{s-1}$, where d is the sum of the digits in the base-s representation of m. Thus, we need only show that

$$\log_s(m+1)\geq\frac{d}{s-1}. \tag{12}$$

To prove (12), we first fix the value of d. We note that the smallest value of m that attains this value of d occurs when all of the base-s digits of m are $s-1$, except for the leading digit, which is, say, ℓ $(0 \le \ell \le s-1)$. We then have that $m+1 = s^w(\ell+1)$ and $d = w(s-1)+\ell$ for some w and ℓ such that $0 \le \ell \le s-1$. We need to show that

$$w + \log_s(\ell+1) = \log_s(s^w(\ell+1)) \ge \frac{w(s-1)+\ell}{s-1} = w + \frac{\ell}{s-1}.$$

Canceling the additive terms of w on each side, all that is left to prove is that

$$\log_s(\ell+1) \ge \frac{\ell}{s-1}. \tag{13}$$

But (13) follows from the concavity of the logarithm function, since equality holds in (13) for $\ell = 0$ and for $\ell = s-1$.

References

[BKS02] P. Bateman, J. Kalb, and A. Stenger, *Problem 10797: A limit involving least common multiples*, Amer. Math. Monthly **109** (2002), 393–394.

[Far05] B. Farhi, *Minorations non triviales du plus petit commun multiple de certaines suites finies d'entiers*, C. R. Acad. Sci. Paris, Ser. I **341** (2005), 469–474.

[Far07] ———, *Nontrivial lower bounds for the least common multiple of some finite sequences of integers*, J. Number Theory **125** (2007), 393–411.

[FK09] B. Farhi and D. Kane, *New results on the least common multiple of consecutive integers*, Proc. Amer. Math. Soc. **137** (2009), 1933–1939.

[Han72] D. Hanson, *On the product of the primes*, Canad. Math. Bull. **15** (1972), 33–37.

[HF06] S. Hong and W. Feng, *Lower bounds for the least common multiple of finite arithmetic progressions*, C.R. Acad. Sci. Paris, Ser. I **343** (2006), 695–698.

[HK10] S. Hong and S. D. Kominers, *Further improvements of lower bounds for the least common multiples of arithmetic progressions*, Proc. Amer. Math. Soc. **138** (2010), 809–813.

[HQ10] S. Hong and G. Qian, *The least common multiple of consecutive terms in arithmetic progressions*, Proc. Edinburgh Math Soc. (2010), in press.

[HY08] S. Hong and Y. Yang, *Improvements of lower bounds for the least common multiple of finite arithmetic progressions*, Proc. Amer. Math. Soc. **136** (2008), 4111–4114.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, 2004.

[Nai82] M. Nair, *On Chebyshev-type inequalities for primes*, Amer. Math. Monthly **89** (1982), 126–129.

[TH10] Q. Tan and S. Hong, *New lower bounds for the least common multiples of arithmetic progressions*, preprint, 2010.

Department of Mathematics, Harvard University
One Oxford Street
Cambridge, MA 02138
E-mail address: dankane@math.harvard.edu, aladkeenin@gmail.com

Department of Economics, Harvard University, and Harvard Business School
Wyss Hall, Harvard Business School
Soldiers Field, Boston, MA 02163
E-mail address: kominers@fas.harvard.edu, skominers@gmail.com