ON ALMOST LEHMER NUMBERS

TOMOHIRO YAMADA

Abstract. We consider composite numbers n such that $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$. We discuss two cases, according to whether the number of prime factors of ℓ is bounded or not. We give a few instances and upper bounds for the number of such integers below a given number.

1. Introduction

1.1. **Backgrounds.** Let

> $\varphi(n)$: the Euler totient of n, the number of positive integers $d \leq n-1$ coprime to n.

Clearly, $\varphi(n) = n-1$ if and only if n is prime.

Then Lehmer Lehmer [8] conjectured that:

Conjecture 1. *There exists no composite n such that*

$$\varphi(n) \mid (n-1). \tag{1.1}$$

Lehmer [8] proved that:

> If n is composite and $\varphi(n)$ divides $n-1$, then n must (a) be odd, (b) be squarefree, and (c) have at least seven prime factors.

Further results:

- Cohen and Hagis [4]: $\omega(n) \geq 14$ and $n > 10^{20}$.
- Renze's notebook [15]: $\omega(n) \geq 15$ and $n > 10^{26}$.
- Pinch claims at his research page [13]: $n > 10^{30}$.

Moreover, letting $V(x)$ be the number of composites $n \leq x$ such that $\varphi(n) \mid (n-1)$,

---

2020 *Mathematics Subject Classification.* Primary 11A25, Secondary 11A05, 11N25.
Key words and phrases. Lehmer's problem, Euler's totient function, multiplicative partition.

- Pomerance [14]: $V(x) = O(x^{1/2}\log^{3/4} x)$ and $n \le r^{2^r}$ if $2 \le \omega(n) \le r$ additionally.
- Luca and Pomerance [9]: $V(x) < x^{1/2}\log^{-1/2+o(1)} x$.
- Burek and Żmija [2]: $n \le 2^{2^r} - 2^{2^{r-1}}$ if $2 \le \omega(n) \le r$ additionally.

Weakening the condition $\varphi(n) \mid (n-1)$, Grau and Oller-Marcén [6] introduced the k-Lehmer property: $\varphi(n) \mid (n-1)^k$

The first few composite 2-Lehmer numbers:

$$561, 1105, 1729, 2465, \ldots$$

(sequence A173703 in OEIS).

Following estimates are known:

- McNew [10]: For each k, the number of k-Lehmer numbers is $O(x^{1-1/(4k-1)})$ and the number of integers which are k-Lehmer for some k is at most $x\exp(-(1+o(1))\log x \log\log\log x/\log\log x)$.
- McNew and Wright [11]: For each $k \ge 3$, there exist at least $x^{1/(k-1)+o(1)}$ integers $n \le x$ which are k-Lehmer but not $(k-1)$-Lehmer.

1.2. **Nearly and almost Lehmer numbers.** Now we would like to discuss intermediate properties between the 1-Lehmer (that is, ordinary Lehmer) property and 2-Lehmer property.

We call an integer n to be

(a) an almost Lehmer number if $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$, and
(b) an r-nearly Lehmer number if $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$ with $\omega(\ell) \le r$.

We begin by noting that:

- The ordinary Lehmer property is equivalent to the 0-nearly Lehmer property and an almost Lehmer numbers can be regarded as ∞-nearly Lehmer numbers.
- The first few almost Lehmer numbers are
  $$1729, 12801, 247105, 1224721, 2704801, 5079361, 8355841, \ldots,$$
  given in A337316.
- There exist exactly 38 almost Lehmer numbers below 2^{32}.
- There exist only five 1-nearly Lehmer numbers 1729, 12801, 5079361, 34479361, and 3069196417 below 2^{32} (further instances are given in the discussion of A338998).

We use the following notion:

- $U_r (r = 1, 2, \ldots, \infty)$: the set of composites n for which $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$ with $\omega(\ell) \leq r$.
- Thus, U_∞ denotes the set of almost Lehmer numbers.
- $S(x) = \{n \leq x, n \in S\}$.

We note that McNew's upper bound for 2-Lehmer numbers immediately yields that $\#U_r(x) \leq \#U_\infty(x) = O(x^{6/7})$.

The purpose of this paper is to give stronger upper bounds for $\#U_r(x)$ and $\#U_\infty(x)$:

Theorem 1 (Yamada [16])**.** *Let a_r be the number of partitions of the multiset $\{1, 1, 2, 2, \ldots, r, r\}$ of r integers repeated twice. Then, there exist two absolute constants c and c_1 such that for each integer $r \geq 1$,*

$$\#U_r(x) < ca_r(x \log x)^{2/3}(c_1 \log \log x)^{2r+2/3}. \tag{1.2}$$

Moreover, we have

$$\#U_\infty(x) < x^{4/5} \exp\left(\left(\frac{4}{5} + o(1)\right) \frac{\log x \log \log \log x}{\log \log x}\right), \tag{1.3}$$

where $o(1) \to 0$ as $x \to \infty$.

The first terms of a_r's are

$$2, 9, 66, 712, 10457, 198091, 4659138, 132315780, \ldots$$

given in A020555 and Bender's asymptotic formula in [1] yields that

$$\log a_r < 2r\left(\log(2r) - \log \log(2r) - 1 - \frac{\log 2}{2} + o(1)\right) \tag{1.4}$$

as r grows.

Hence, setting c and c_1 as in Theorem 1, we have

Corollary 2 (Yamada [16])**.**

$$\#U_1(x) < 2c(x \log x)^{2/3}(c_1 \log \log x)^{2r+2/3} \tag{1.5}$$

and

$$\#U_r(x) < \left(\frac{(e\sqrt{2} + o_r(1))r}{\log r}\right)^{2r} (x \log x)^{2/3}(c_1 \log \log x)^{2r+2/3}, \tag{1.6}$$

where $o_r(1)$ tends to zero as r tends to infinity.

Our estimates depend on numbers of multiplicative partitions of integers, which will be discussed in the next section.

This dependence, together with factorial growth of a_r, prevents our method from showing that $\#U_\infty(x) < x^{2/3+o(1)}$.

On the other hand, the above instances lead us to:

Conjecture 2. *There exist infinitely many almost Lehmer composite numbers.*

Moreover, there may be infinitely many 1-nearly Lehmer composite numbers (it may occur that $\#U_1(x) \gg \log x$), although such integers are distributed very rarely below our search limit.

However, these also seem to be difficult to prove or disprove; it is even not known whether there exist infinitely many 2-Lehmer numbers or not!

2. Preliminary estimates

Let $\tau(s)$ be the number of multiplicative partitions / factorizations of $s = s_1 s_2 \cdots s_r$ with $s_1 \leq s_2 \leq \cdots s_r$.

The values of $\tau(s)$ for positive integers s are given in A001055.

Example 1. *If $s = p_1^2 p_2^2$, then there exist nine factorizations: $\{p_1^2 p_2^2\}$, $\{p_1^2 p_2, p_2\}$, $\{p_1 p_2^2, p_1\}$, $\{p_1^2, p_2^2\}$, $\{p_1^2, p_2, p_2\}$, $\{p_2^2, p_1, p_1\}$, $\{p_1 p_2, p_1 p_2\}$, $\{p_1 p_2, p_1, p_2\}$, $\{p_1, p_1, p_2, p_2\}$.*

We prove two lemmas.

Lemma 3. *For each integer $s \geq 1$, let $S(s; x)$ denote the set of positive integers $n \leq x$ such that s divides $\varphi(n)$. Then*

$$S(s; x) \leq \frac{\tau(s) x (c_1 \log\log x)^{\Omega(s)}}{s}, \tag{2.1}$$

where c_1 is an absolute constant.

Lemma 4. *As x tends to infinity, we have*

$$\sum_{s \leq x} \frac{\tau(s)}{s} < \frac{(1 + o(1)) e^{2\sqrt{\log x}} \log^{1/4} x}{2\sqrt{\pi}}. \tag{2.2}$$

Lemma 3 follows from

Lemma 5 (Erdős, Granville, Pomerance, and Spiro[5])**.**

$$\sum_{q \leq x, q \equiv 1 \pmod{s}} \frac{1}{q} < \frac{c_1 \log\log x}{s} \tag{2.3}$$

with some absolute constant c_1, where q runs over all primes satisfying $q \leq x, q \equiv 1 \pmod{s}$.

Lemma 4 immediately follows from

Lemma 6 (Oppenheim[12])**.**

$$\sum_{s\leq x}\tau(s)=\frac{(1+o(1))xe^{2\sqrt{\log x}}}{2\sqrt{\pi}\log^{3/4}x}. \tag{2.4}$$

Note: $\tau(s)$ itself may be fairly large.

Indeed, Canfield, Erdős, and Pomerance [3] showed that $\tau(s)=s\exp(-(1+o(1))\log s\log\log\log s/\log\log s)$ for highly factorable integers s, which are given in A033833.

So that, the above lemma cannot be used in order to bound the number of integers n such that $\varphi(n)$ are multiples of s for an arbitrary integer s. Nevertheless, we can show the following upper bound for a certain sum involving $\tau(s)$, as we have done in Lemma 4.

3. Proof of the theorem

- r: a positive integer or ∞,
- x: a sufficiently large real number,
- n: be an r-nearly Lehmer number $\leq x$ which is composite.

Clearly, we can write $(n-1)/\varphi(n)=k/\ell$, where

- k and ℓ: coprime integers,
- ℓ: a squarefree divisor of $n-1$ with $\omega(\ell)\leq r$,
- $\ell_0=\gcd(\ell,\varphi(d))$, $\ell_2=\prod_{p\mid\ell_0,p^2\mid\varphi(d)}p$.

We note that n must be odd and squarefree since $\varphi(n)$ and n are coprime and n is composite.

Take an arbitrary divisor d of n and write $n=md$. Since n is squarefree, we have $\ell(md-1)=k\varphi(n)=k\varphi(m)\varphi(d)$. Thus we obtain

$$md\equiv 1\left(\operatorname{mod}\frac{\varphi(d)}{\ell_2}\right) \tag{3.1}$$

since $md\equiv 1\left(\operatorname{mod}\frac{\varphi(d)}{\ell_0}\right)$ but both $\varphi(d)/\ell_0$ and ℓ_0 divide $md-1$.

Now let $L_1>x^{1/3}$ and $L_2=L_1^2$ be real numbers which will be chosen later in different manners according to whether r is an integer or $r=\infty$. We cannot have $n=mp$ for a prime $p>L_2$; $m\equiv 1\pmod{(p-1)/\ell_2}$ for some $\ell_2^2\mid(p-1)$ from the first observation, $m>\sqrt{p}$, and $n>p^{3/2}>L_2^{3/2}=L_1^3$, which is a contradiction. Thus, we observe that n has a divisor d in the range $L_1\leq d\leq L_2$ if $n\geq L_1$.

For each d, the number of integers $n = md \leq x$ satisfying (3.1) is at most $1 + \lfloor \ell_2 x/(d\varphi(d)) \rfloor$. We note that $\ell_2 \leq \sqrt{\varphi(d)} \leq L_1$. Moreover, we have $d/\varphi(d) \ll \log\log d \leq \log\log x$, which follows from Theorem 328 of Hardy and Wright [7].

3.1. If $r < \infty$, then $\tau(\ell_2^2) \leq \tau(\ell^2) \leq a_r$. By Lemma 3, we have

$$
\begin{aligned}
\#U_r(x) &\leq L_1 + \sum_{\ell_2 \leq L_1} \sum_{\substack{L_1 \leq d \leq L_2,\\ \ell_2^2 \mid \varphi(d)}} \left(1 + \frac{\ell_2 x}{d\varphi(d)}\right) \\
&\ll \sum_{\ell_2 \leq L_1} \left(\#S(\ell_2^2; L_2) + \sum_{L_1 \leq d \leq L_2, \ell_2^2 \mid \varphi(d)} \frac{\ell_2 x \log\log x}{d^2} \right) \\
&\ll a_r \sum_{\ell_2 \leq L_1} \left(\frac{L_2 (c_1 \log\log x)^{\Omega(\ell_2^2)}}{\ell_2^2} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2^2)+1}}{L_1 \ell_2} \right) \\
&\ll a_r \left(L_2 (c_1 \log\log x)^{2r} + \frac{x (\log x)(c_1 \log\log x)^{2r+1}}{L_1} \right).
\end{aligned}
\tag{3.2}
$$

Taking $L_1 = (c_1 x \log x \log\log x)^{1/3}$, we obtain the theorem.

3.2. Now assume that $r = \infty$. Instead of (3.2), we obtain

$$
\begin{aligned}
\#U_\infty(x) &\ll \sum_{\ell_2 < L_1} \left(\#S(\ell_2^2; L_2) + \sum_{L_1 \leq d \leq L_2, \ell_2^2 \mid \varphi(d)} \frac{x (\log\log x)^{1/2}}{d^{3/2}} \right) \\
&\ll \sum_{\ell_2 \leq L_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \left(L_2 (c_1 \log\log x)^{\Omega(\ell_2)} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2)+1/2}}{L_1^{1/2}} \right),
\end{aligned}
\tag{3.3}
$$

observing that since $\ell_2^2 \mid \varphi(d)$, we have $\varphi(d)/\ell_2 \geq \sqrt{\varphi(d)} \gg (d/\log\log d)^{1/2}$ using Theorem 328 of Hardy and Wright [7] again.

Since $\ell_2 < L_2^{1/2}$, $\Omega(\ell_2^2) = 2\omega(\ell_2) < (1 + o(1)) \log L_2 / \log\log x$ from Hardy and Wright [7, Chapter 22.10]. By Lemma 4, we have $\sum_{\ell_2 < L_1} \tau(\ell_2^2)/\ell_2^2 \ll e^{2\sqrt{\log x}} \log^{1/4} x$. Thus, (3.3) gives that

$$
\#U_\infty(x) \ll e^{(1+o(1)) \log L_2 \log\log\log x / \log\log x} \left(L_2 + \frac{x}{L_1^{1/2}} \right). \tag{3.4}
$$

Now the theorem immediately follows taking $L_1 = x^{2/5}$. This completes the proof.

References

[1] Edward A. Bender, Partitions of multisets, *Discrete Math.* **9** (1974), 301–311.

[2] Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, *Int. J. Number Theory* **15** (2016), 1463–1468.

[3] E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", *J. Number Theory* **17** (1983), 1–28.

[4] G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, *Nieuw Arch. Wisk.* (3) **28** (1980), 177–185.

[5] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, in Bruce C. Berndt, Harold G. Diamond, Heini Halberstam, and Adolf Hildebrand, eds., *Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman*, Birkhäuser, 1990, pp. 165–204.

[6] José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, *Integers* **12** (2012), #A37.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

[8] D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932), 745–751.

[9] Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, *Bol. Soc. Mat. Mexicana* (3) **17** (2011), 13–21.

[10] Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, *Int. J. Number Theory* **9** (2013), 1215–1224.

[11] Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, *Int. J. Number Theory* **12** (2016), 1863–1869.

[12] A. Oppenheim, On an arithmetic function II, *J. London Math. Soc.* **2** (1927), 123–130.

[13] Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

[14] Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, *Pacific J. Math.* **69** (1977), 177–186.

[15] John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

[16] Tomohiro Yamada, On almost Lehmer numbers, *J. Integer Seq.* **24** (2021), Article 21.5.5.

Center for Japanese language and culture, Osaka University, 562-8558, 8-1-1, Aomatanihigashi, Minoo, Osaka, Japan

Email address: `tyamada1093@gmail.com`