Journal of Integer Sequences, Vol. 24 (2021),
Article 21.5.5

On Almost Lehmer Numbers

Tomohiro Yamada
Center for Japanese Language and Culture
Osaka University
562-8558, 8-1-1, Aomatanihigashi
Minoo, Osaka
Japan
tyamada1093@gmail.com

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

Let $\varphi(n)$ denote the Euler totient function of n. Clearly, $\varphi(p) = p-1$ for any prime p. Lehmer [8] conjectured that there exists no composite number n such that $\varphi(n)$ divides $n-1$ and showed that such an integer must be an odd squarefree integer with at least seven prime factors. In other words, if $\varphi(n) \mid (n-1)$ and n is composite, then n is odd and $\omega(n) = \Omega(n) \geq 7$, where $\omega(n)$ and $\Omega(n)$ respectively denote the number of distinct and not necessarily distinct prime factors of n.

For such an integer n, Cohen and Hagis [4] showed that $\omega(n) \geq 14$ and $n > 10^{20}$, Renze's notebook [15] shows that $\omega(n) \geq 15$ and $n > 10^{26}$, and Pinch claims that $n > 10^{30}$ at his research page [13]. Pomerance [14] showed that the number of such an integer $n \leq x$ is $O(x^{1/2}\log^{3/4} x)$ and $n \leq r^{2^r}$ if $2 \leq \omega(n) \leq r$ additionally. Luca and Pomerance [9] showed that the number of such an integer $n \leq x$ is at most

$$\frac{x^{1/2}}{\log^{1/2+o(1)} x}.$$

Furthermore, Burek and Żmija [2] showed that $n \leq 2^{2^r} - 2^{2^{r-1}}$ if $\varphi(n)$ divides $n-1$ and $2 \leq \omega(n) \leq r$.

Weakening the condition $\varphi(n) \mid (n-1)$, Grau and Oller-Marcén [6] introduced the k-Lehmer property that $\varphi(n) \mid (n-1)^k$ and called a composite number with this property to be a k-Lehmer number. The first few 2-Lehmer numbers are $561, 1105, 1729, 2465, \ldots$ (sequence A173703). McNew [10] showed that 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 numbers for some k is at most $x \exp(-(1+o(1)) \log x \log\log\log x / \log\log x)$. McNew and Wright [11] showed that for each $k \geq 3$, there exist at least $x^{1/(k-1)+o(1)}$ integers $n \leq x$ which are k-Lehmer but not $(k-1)$-Lehmer numbers.

In this paper, we would like to discuss intermediate properties between the 1-Lehmer (that is, ordinary Lehmer) property and 2-Lehmer property.

We call a composite number n to be an almost Lehmer number if $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$ and an r-nearly Lehmer number if $\varphi(n)$ divides $\ell(n-1)$ for some squarefree divisor ℓ of $n-1$ with $\omega(\ell) \leq r$. The ordinary Lehmer property is equivalent to the 0-nearly Lehmer property and an almost Lehmer number can be called an ∞-nearly Lehmer number.

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} as given in A338998.

For $r = 1, 2, \ldots, \infty$, let U_r be the set of composite numbers 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. We also use the general notion that $S(x) = \{n \leq x, n \in S\}$ denote the set of integers S up to x for a set S of positive integers. Then 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. *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 $r \geq 1$,*

$$\#U_r(x) < c a_r (x \log x)^{2/3} (c_1 \log\log x)^{2r+2/3}. \tag{1}$$

Moreover, we have

$$\#U_\infty(x) < x^{4/5} \exp\left(\left(\frac{4}{5} + o(1)\right) \frac{\log x \log\log\log x}{\log\log x}\right), \tag{2}$$

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

The first few terms of the sequence (a_r) are $2, 9, 66, 712, 10457, \ldots$ given in A020555. Bender's asymptotic formula [1, Theorem 1] yields that

$$\log a_r < 2r\left(\log(2r) - \log\log(2r) - 1 - \frac{\log 2}{2} + o(1)\right) \tag{3}$$

as r grows. Hence, we obtain the following estimates.

Corollary 2. *Setting c and c_1 as in Theorem 1, we have*

$$\#U_1(x) < 2c(x\log x)^{2/3}(c_1 \log\log x)^{2r+2/3} \tag{4}$$

and

$$\#U_r(x) < \left(\frac{(e\sqrt{2} + o_r(1))r}{\log r}\right)^{2r} (x\log x)^{2/3}(c_1\log\log x)^{2r+2/3}, \tag{5}$$

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. Thus, fast growth of a_r prevents us from showing that $\#U_\infty(x) < x^{2/3+o(1)}$.

On the other hand, the above instances lead us to conjecture that there exist infinitely many almost Lehmer numbers. Moreover, there may be infinitely many 1-nearly Lehmer numbers, 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 of $s = s_1 s_2 \cdots s_r$ with $s_1 \le s_2 \le \cdots \le s_r$. The values of $\tau(s)$ for positive integers s are given in A001055.

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

$$\#S(s;x) \le \frac{\tau(s)x(c_1\log\log x)^{\Omega(s)}}{s}, \tag{6}$$

where c_1 is an absolute constant.

Proof. We observe that if $s \mid \varphi(n)$, then $q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t} q_{t+1} \cdots q_r \mid n$ for some integers $f_1, f_2, \ldots, f_t \ge 2$ and distinct primes $q_1, q_2, \ldots, q_r$ such that

$$s \mid q_1^{f_1-1} q_2^{f_2-1} \cdots q_t^{f_t-1}(q_1-1)(q_2-1)\cdots(q_r-1).$$

Moreover, we can take such q_i's in the way that there exists a factorization of $s = s_1 s_2 \cdots s_{r+1}$ with $1 < s_1 \le s_2 \le \cdots \le s_r$ such that $q_i \equiv 1 \pmod{s_i}$ for $i = 1, 2, \ldots, r$ and s_{r+1} divides $q_1^{f_1-1} q_2^{f_2-1} \cdots q_t^{f_t-1}$.

For each factorization $s = s_1 s_2 \cdots s_{r+1}$, the number of such integers $n \le x$ does not exceed

$$\sum_{\substack{q_i \le x,\\ q_i \equiv 1 \pmod{s_i} (i=1,2,\ldots,r)}} \frac{x}{q_1 q_2 \cdots q_r s_{r+1}} = \frac{x}{s_{r+1}} \prod_{i=1}^{r} \left(\sum_{\substack{q_i \le x,\\ q_i \equiv 1 \pmod{s_i}}} \frac{1}{q_i} \right).$$

We obtain from Erdős, Granville, Pomerance, and Spiro [5, (3.1)] that for $i = 1, 2, \ldots, r$,

$$\sum_{\substack{q_i \le x,\\ q_i \equiv 1 \pmod{s_i}}} \frac{1}{q_i} < \frac{c_1 \log\log x}{s_i} \tag{7}$$

with some absolute constant c_1. Thus, we conclude that the number of integers $n \le x$ such that s divides $\varphi(n)$ corresponding to each factorization $s = s_1 s_2 \cdots s_{r+1}$ can be bounded from above by

$$\frac{x(c_1 \log\log x)^r}{s_1 s_2 \cdots s_r s_{r+1}} = \frac{x(c_1 \log\log x)^r}{s}.$$

Now the lemma immediately follows noting that $r \le \Omega(s)$. ☐

We must note that although $\tau(s)$ is relatively small when $\Omega(s)$ is small but not when $\Omega(s)$ is 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 $\tau(s)$.

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

$$\sum_{s \le x} \frac{\tau(s)}{s} < \frac{(1 + o(1)) e^{2\sqrt{\log x}} \log^{1/4} x}{2\sqrt{\pi}}. \tag{8}$$

Proof. Oppenheim [12] proved that

$$\sum_{s \le x} \tau(s) = \frac{(1 + o(1)) x e^{2\sqrt{\log x}}}{2\sqrt{\pi} \log^{3/4} x}. \tag{9}$$

By partial summation, we immediately obtain (8). ☐

3 Proof of the theorem

Let r be a positive integer or ∞, x denotes a sufficiently large real number, and $n \le x$ be an r-nearly Lehmer number. In this section, the implied constants in $\ll$ and the O-symbols are absolute and each $o(1)$ tends to zero as x goes to infinity.

We begin by writing $(n-1)/\varphi(n) = k/\ell$, where k and ℓ are coprime integers and ℓ is a squarefree integer with at most r distinct prime factors dividing $n-1$. 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 $\ell(md-1) = k\varphi(n) = k\varphi(m)\varphi(d)$ and

$$md \equiv 1 \pmod{\frac{\varphi(d)}{\ell_0}}, \tag{10}$$

where $\ell_0 = \gcd(\ell, \varphi(d))$.

It is clear that $\ell_0 \mid \ell \mid (n-1)$ and therefore both $\varphi(d)/\ell_0$ and ℓ_0 divide $md-1$. Let $a \mid\mid b$ denote that $a \mid b$ and $\gcd(a, b/a) = 1$. We observe that if $p^e \mid\mid \varphi(d)$, then $p^{e-1} \mid \varphi(d)/\ell_0 \mid (md-1)$ and if $p \mid\mid \varphi(d)$, then $p \mid \varphi(d) \mid \ell(n-1) \mid (n-1)^2 = (md-1)^2$ and therefore $p \mid (md-1)$. Hence, decomposing $\ell_0 = \ell_1\ell_2$, where each prime factor p of ℓ_0 divides ℓ_1 if and only if $p \mid\mid \varphi(d)$, we obtain

$$md \equiv 1 \pmod{\frac{\varphi(d)}{\ell_2}}. \tag{11}$$

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 can easily see that n cannot have a prime factor $p > L_2$. If $n = mp$ with $p > L_2$, then the above observation yields that $mp \equiv 1 \pmod{(p-1)/\ell_2}$. Since $p \equiv 1 \pmod{(p-1)/\ell_2}$ clearly, we have $m \equiv 1 \pmod{(p-1)/\ell_2}$ and therefore $m \ge (p-1)/\ell_2$. However, we see that $p \equiv 1 \pmod{\ell_2^2}$ since $\ell_2^2 \mid \varphi(p) = p-1$. Thus, we must have $p < m^2 = (n/p)^2 < (x/p)^2$ and $p < x^{2/3} \le L_2$, which is a contradiction.

Hence, n must have a prime factor $p \le L_2$. If $n \ge L_1$ and n has no prime divisor $p \ge L_1$, then the smallest divisor $d \ge L_1$ of n must satisfy $L_1 \le d \le L_1^2 = L_2$. Clearly, if n has a prime factor p in the range $L_1 \le d \le L_2$, then n has a divisor $d = p$ with $L_1 \le d \le L_2$. Thus, we observe that n has a divisor d in the range $L_1 \le d \le L_2$ if $n \ge L_1$.

For each d, the number of integers $n = md \le x$ satisfying (11) is at most $1 + \lfloor \ell_2 x/(d\varphi(d)) \rfloor$. We note that $\ell_2 \le \sqrt{\varphi(d)} \le L_1$. Hence, using the inequality $d/\varphi(d) \ll \log\log d \le \log\log x$, which follows from Theorem 328 of Hardy and Wright [7], we have

$$\begin{aligned} \#U_r(x) &\le L_1 + \sum_{\ell_2 \le L_1} \sum_{\substack{L_1 \le d \le L_2, \\ \ell_2^2 \mid \varphi(d)}} \left(1 + \frac{\ell_2 x}{d\varphi(d)}\right) \\ &\ll \sum_{\ell_2 \le L_1} \left(\#S(\ell_2^2; L_2) + \sum_{\substack{L_1 \le d \le L_2, \\ \ell_2^2 \mid \varphi(d)}} \frac{\ell_2 x \log\log x}{d^2} \right). \end{aligned} \tag{12}$$

Let us estimate $\#U_r(x)$ for $r < \infty$. Recalling the definition of a_r, it is clear that $\tau(s^2) = a_{\omega(s)}$ for any squarefree integer s. Thus, we have $\tau(\ell_2^2) \le \tau(\ell^2) \le a_r$. Using Lemma 3 and partial summation, we obtain

$$\begin{aligned}\#U_r(x) &\ll a_r \sum_{\ell_2 \le L_1} \left(\frac{L_2 (c_1 \log\log x)^{\Omega(\ell_2^2)}}{\ell_2^2} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2^2)+1}}{L_1 \ell_2} \right) \\ &\ll a_r \left(L_2 (c_1 \log\log x)^{2r} + \frac{x (\log x)(c_1 \log\log x)^{2r+1}}{L_1} \right).\end{aligned} \tag{13}$$

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

Finally, we shall estimate $\#U_\infty(x)$. Since $\ell_2^2 \mid \varphi(d)$, we have $\varphi(d)/\ell_2 \ge \sqrt{\varphi(d)} \gg (d/\log\log d)^{1/2}$ using Theorem 328 of Hardy and Wright [7] again. Now, instead of the bottom line of (12), we obtain

$$\begin{aligned}\#U_\infty(x) &\ll \sum_{\ell_2 < L_1} \left(\#S(\ell_2^2; L_2) + \sum_{\substack{L_1 \le d \le L_2, \\ \ell_2^2 \mid \varphi(d)}} \frac{x (\log\log x)^{1/2}}{d^{3/2}} \right) \\ &\ll \sum_{\ell_2 \le L_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \left(L_2 (c_1 \log\log x)^{\Omega(\ell_2)} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2)+1/2}}{L_1^{1/2}} \right).\end{aligned} \tag{14}$$

Since ℓ_2 is squarefree, we have $\Omega(\ell_2^2) = 2\omega(\ell_2)$. Hence, from Hardy and Wright [7, Chapter 22.10], we see that

$$\Omega(\ell_2^2) < \frac{2(1 + o_{\ell_2}(1)) \log \ell_2}{\log\log \ell_2} < \frac{(1 + o(1)) \log L_2}{\log\log x}, \tag{15}$$

where the former $o_{\ell_2}(1)$ tends to zero as ℓ_2 goes to infinity but the latter $o(1)$ tends to zero as L_2 (and therefore x) goes to infinity. By Lemma 4, we have

$$\sum_{\ell_2 < L_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \le \sum_{s < L_2} \frac{\tau(s)}{s} \ll e^{2\sqrt{\log x}} \log^{1/4} x. \tag{16}$$

Inserting (15) and (16) into (14), we obtain

$$\#U_\infty(x) \ll e^{(1+o(1)) \log L_2 \log\log\log x / \log\log x} \left(L_2 + \frac{x}{L_1^{1/2}} \right). \tag{17}$$

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*, *Progr. Math.*, Vol. 85, 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, 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/.

2020 *Mathematics Subject Classification*: Primary 11A25; Secondary 11A05, 11N25.
Keywords: Lehmer's problem, Euler's totient function, multiplicative partition.

(Concerned with sequences A001055, A020555, A033833, A173703, A337316, and A338998.)

Received November 24 2020; revised versions received November 25 2020; February 25 2021.
Published in *Journal of Integer Sequences*, April 25 2021.

Return to Journal of Integer Sequences home page.