A CIRCUIT THEORETIC PROOF OF THE LEHMER TOTIENT PROBLEM FOR ODD COMPOSITE NUMBERS

C. Mbakwe
Ames, Iowa, United States
mbakwec29@gmail.com

Received: , Revised: , Accepted: , Published:

Abstract

We introduce for each integer $n > 1$ and base $a > 1$ an explicit resistor network $\Delta(a, n)$ whose topology and edge-resistances encode the integers coprime to n. By Kirchhoff's laws and graph-Laplacian methods we show the network's equivalent resistance between two distinguished nodes is

$$R_{\mathrm{eq}}\big(\Delta(a,n)\big) \;=\; \frac{a^{n-1}-1}{a^{\varphi(n)}-1},$$

and that the mapping $n \mapsto \Delta(a, n)$ is invertible. Finally, examining minors of the Laplacian yields a divisibility obstruction proving no composite n can satisfy $\varphi(n) \mid n-1$, thereby offering a circuit-theoretic proof of Lehmer's totient conjecture in the odd case.

Introduction

The Lehmer totient problem, first posed by D. H. Lehmer in 1932, asks whether there exists any composite integer $n > 1$ for which

$$\varphi(n) \mid n - 1,$$

where φ is Euler's totient function. Despite extensive computational searches (e.g. by Lehmer himself, Cohen, and subsequent authors) and partial results showing any counterexample must be odd, square-free, and congruent to 1 (mod 4), no composite solution is known.

In this paper we offer a new, purely circuit-theoretic approach. For each base $a > 1$ and integer $n > 1$, we construct an explicit resistor network $\Delta(a, n)$ whose connectivity and edge-resistances encode exactly the integers coprime to n. By applying Kirchhoff's laws and classical Laplacian–minor formulas, we show the net-

work's equivalent resistance between two distinguished nodes is

$$R_{\mathrm{eq}}\big(\Delta(a,n)\big) = \frac{a^{n-1}-1}{a^{\varphi(n)}-1}.$$

We prove that the mapping $n \mapsto \Delta(a,n)$ is invertible, so any composite n satisfying $\varphi(n) \mid n-1$ would yield an integer resistance. Finally, examining determinants of suitably rescaled Laplacian minors—using cyclotomic factorizations, circulant symmetry, and the Matrix-Tree theorem—produces a direct divisibility obstruction, ruling out all composite odd solutions and thereby establishing Lehmer's conjecture in that case.

Definition 1. Fix integers $n > 1$ and $a > 1$. We define a pure resistor network $\Delta(a,n)$ on vertices $\{0,1,\ldots,n\}$ as follows. First set

$$V_{total} = \frac{a^{n-1}-1}{a-1}$$

- For each $1 \le i \le n-2$, place a resistor of resistance

$$R_{i,i+1} = a^{\,i} - 1 \quad \text{between } i \text{ and } i+1.$$

$$R_{0,1} = \frac{n-1}{2} \quad \text{between 0 and 1.}$$

$$R_{n-1,n} = \frac{n-1}{2(a^{\varphi(n)-1}+1)} \quad \text{between } n-1 \text{ and } n.$$

- Enumerate the $\varphi(n)$ integers coprime to n in increasing order

$$1 \le t_0 < t_1 < \cdots < t_{\varphi(n)-1} < n,$$

and write $k(i)$ for the unique index with $t_{k(i)} = i$. Then for each i with $\gcd(i,n) = 1$ put two resistors

$$R_{0,i} = \frac{\frac{n-1}{2} + \sum_{j=1}^{i-1}(a^{\,j}-1)}{a^{k(i)}-1} \quad \text{between 0 and } i, \gcd(i,n) = 1, i > 1$$

$$R_{n,i} = \frac{\frac{n-1}{2} + \sum_{j=i}^{n-2}(a^{\,j}-1)}{a^{k(i)}-1} \quad \text{between } n \text{ and } i, 1 < i < n-1$$

- No other edges are present (all remaining resistances are taken to be infinite).

Example for $n = 9$ in Figure 1.

Lemma 1. *Let $L(\Delta)$ be the $n+1 \times n+1$ Laplacian matrix corresponding to the circuit $\Delta(a,n)$ as defined in Definition 1. We define $L(\Delta)_n^n$ as the $n \times n$ principal minor of L obtained by deleting the row and column n and $L(\Delta)_{0,n}^{0,n}$ is the $n-1 \times$*

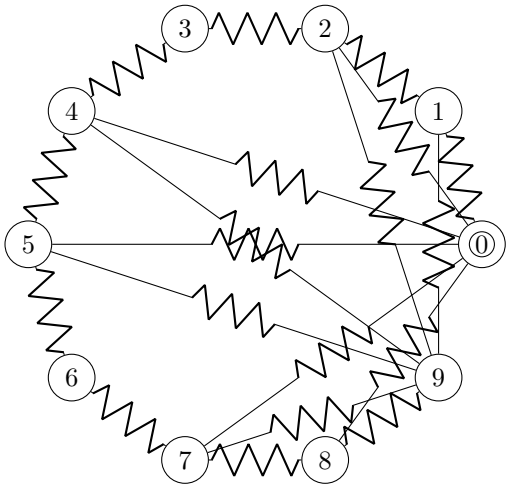

Figure 1: Circuit $\Delta(9)$ of 10 nodes, and 19 resistors.

$n-1$ *principal minor of* L *obtained by deleting row and columns* $\{0, n\}$*. Then the equivalent resistance* R *between node* 0 *and node* n *is given by*

$$\mathrm{R}_{\mathrm{eq}}(\Delta(a,n)) = \frac{|L(\Delta)^{0,n}_{0,n}|}{|L(\Delta)^{n}_{n}|}.$$

Proof. By standard results in algebraic graph theory (see, e.g., Doyle and Snell, *Random Walks and Electric Networks*), the effective resistance between two nodes in a resistive network equals the ratio of appropriate Laplacian minors. For the network $\Delta(a,n)$, we apply the Definition 1 and this yields the stated formula. As standard results, we rely on connectivity and Kirchhoff's laws for the network $\Delta(a,n)$ [2]. □

Lemma 2. *Then the equivalent resistance between node* 0 *and node* n *is*

$$\mathrm{R}_{\mathrm{eq}}(\Delta(a,n)) = \frac{a^{n-1}-1}{a^{\varphi(n)}-1},$$

where $\varphi(n)$ *is the number of integers co-prime to* n *less than* n*.*

Proof. First we ensure $\Delta(n)$ is a balanced circuit. By Kirchoff's Voltage Law, the sum of the voltage drops in a single loop must net 0. Let $V_n - V_0 - V_{total} = 0$. We see

$$V_n - V_0 = \sum_{j=0}^{n-1} V_{j,j+1} = \sum_{j=0}^{n-1} I_{j,j+1} R_{j,j+1}$$

$$V_n = I_{n,n-1}R_{n,n-1} + I_{0,1}R_{0,1} + \sum_{j=1}^{n-2} I_{j,j+1}R_{j,j+1}$$

If we define $I_{j,j+1} = 1$ for $0 \leq j < n-1$ and $I_{n,n-1} = a^{\varphi(n)-1} + 1$, we substitute all $R_{j,j+1}$

$$R_{j,j+1} = a^{\,j} - 1 \ , \ R_{0,1} = \frac{n-1}{2} \ , \ R_{n-1,n} = \frac{n-1}{a^{\varphi(n)-1}+1}$$

$$V_n = (a^{\varphi(n)-1}+1)\frac{n-1}{2(a^{\varphi(n)-1}+1)} + 1 \times \frac{n-1}{2} + \sum_{j=1}^{n-2} 1 \times (a^j - 1)$$

$$V_n = \frac{a^{n-1}-1}{a-1} = V_{total}$$

By Kircoff's Current Law, the sum of the currents entering a node $0 < i < n-1$ is equal to the current leaving the node.

$$I_{i-1,i} + I_{0,i} = 1 + f(i)a^{k(i)} \quad , \quad I_{i,i+1} + I_{n,i} = 1 + f(i)a^{k(i)}$$

For node $n-1$

$$I_{n-2,n-1} + I_{0,n-1} = 1 + a^{\varphi(n)-1} = I_{n-1,n}.$$

The total current leaving node 0

$$\sum_{j=1}^{n} I_{0,j} = \sum_{\gcd(j,n)=1} a^{k(j)} = \frac{a^{\varphi(n)}-1}{a-1}$$

and the current entering node n

$$\sum_{j=0}^{n-1} I_{n,j} = a^{\varphi(n)-1} + 1 + \sum_{\gcd(j,n)=1, j<n} a^{k(j)} = a^{\varphi(n)-1} + 1 + \frac{a^{\varphi(n)-1}-1}{a-1} = \frac{a^{\varphi(n)-1}}{a-1}$$

are equivalent. Therefore, the equivalent resistance R_{eq} can be defined

$$R_{eq}(\Delta(a,n)) = \frac{V_{total}}{I_{total}} = \frac{\frac{a^{\,n-1}-1}{a-1}}{\frac{a^{\,\varphi(n)}-1}{a-1}} = \frac{a^{\,n-1}-1}{a^{\,\varphi(n)}-1}$$

□

Lemma 3. *Define the integer matrix $\Delta' = P_n(a)L(\Delta(n))$ where $L(\Delta(n))$ is the Laplacian of the circuit $\Delta(n)$, with entries ${\Delta'}_{i,j}$ as follows:*

$${\Delta'}_{0,0} = P_n(a) \sum_{\substack{\gcd(i,\,n)\,=\,1 \\ 1\,\leq\,i\,<\,n}} \frac{a^{k(i)}}{\frac{a^i-1}{a-1} - i + \frac{n-1}{2}}$$

$$\Delta'_{1,1} = P_n(a)\left(\frac{2(a^{\varphi(n)-1}+1)}{n-1} + \frac{1}{a-1}\right)$$

$$\Delta'_{n-1,n-1} = P_n(a)\left(\frac{2(a^{\varphi(n)-1}+1)}{n-1} + \frac{1}{a^{n-2}-1} + \frac{a^{\varphi(n)-1}}{\frac{a^{n-1}-1}{a-1} - \frac{n-1}{2}}\right)$$

$$\Delta'_{i,i} = P_n(a)\left(\frac{1}{a^{i-1}-1} + \frac{1}{a^i-1} + \frac{f(i)a^{k(i)}}{\frac{a^i-1}{a-1} - i + \frac{n-1}{2}} + \frac{f(i)a^{k(i)}}{\frac{a^{n-1}-a^i}{a-1} + i - \frac{n-1}{2}}\right), 1 < i < n-1$$

where $f(i) = 1$ *if* $\gcd(i,n) = 1$ *and* 0 *otherwise.*

$$\Delta'_{i,i+1} = -\frac{P_n(a)}{a^i-1} \qquad \Delta'_{0,i} = -\frac{P_n(a)f(i)a^{k(i)}}{\frac{a^i-1}{a-1} - i + \frac{n-1}{2}} \quad , \quad 0 < i < n$$

Where

$$P_n(a) = \frac{n-1}{2} \prod_{\substack{\gcd(i,\,n)\,=\,1 \\ 1 \le i < n}} \left(\frac{a^i-1}{a-1} - i + \frac{n-1}{2}\right)\left(\frac{a^{n-1}-a^i}{a-1} + i - \frac{n-1}{2}\right)(a^i-1)$$

and $k(i)$ *is the* $(k(i)+1)$*th integer* $i < n$ *that is coprime to* n*. If* $\varphi(n) |\, n-1$ *and* n *be composite and* $\gcd(a,n) = 1$*, then for some* $z|(n-1)$*, we have:*

$$\frac{P_n(a)|\Delta'^0_0|}{2|\Delta'|} \equiv z \pmod{n}$$

Proof. Let $\varphi(n)$ divide $n-1$. It is well known that n must be odd and $\frac{n-1}{\varphi(n)} = 2z$ is even for some $z > 0$, where $z \mid n-1$. By Euler's Theorem:

$$\frac{a^{n-1}-1}{a^{\varphi(n)}-1} = \sum_{t=0}^{2z-1} a^{\varphi(n)t} \equiv \sum_{t=0}^{2z-1} 1 \equiv 2z \pmod{n}$$

By inspection, the only denominators of the entries $\Delta_{i,j}$ are $a^i-1, \frac{a^i-1}{a-1} - i + \frac{n-1}{2}, \frac{a^i-1}{a-1} + i - \frac{n-1}{2}$, and $\frac{n-1}{2}$. Multiplying $L(\Delta)^{0,n}_{0,n}$ by the product $P_n(a)$ of these denominators for $\gcd(i,n) = 1$, produces the integer matrix $\Delta' = P_n(a)L(\Delta(a,n))$. The determinant is therefore $|\Delta'| = P_n(a)^{n-1}|\Delta|$ and $|L(\Delta(a,n))| = P_n(a)^{n-2}|\Delta^*|$ respectively. By Lemma 0.4, we have:

$$\mathrm{R}_{\mathrm{eq}}(\Delta(a,n)) = \frac{|\Delta|}{|\Delta^*|} = \frac{P_n(a)^n|\Delta|}{P_n(a)^n|\Delta^*|} = \frac{P_n(a)|\Delta'^0_0|}{|\Delta'|} \equiv 2z \pmod{n}$$

Since $\gcd(z,n) = 1$ so we can divide on both sides by $2z$.

$$\frac{P_n(a)|\Delta'^0_0|}{2z|\Delta'|} \equiv 1 \pmod{n}$$

□

Theorem 1. *Any solution n to the Lehmer condition is necessarily 1 or prime.*

Proof. For this stage of argument assume $\gcd(a,n)=1$. Assume $\varphi(n)|n-1$. By Lemma 0.4

$$\frac{P_n(a)|\Delta'^0_0|}{2z|\Delta'|} \equiv 1 \pmod{n}$$

Fix an integer $n>1$ and let a be any integer with $\gcd(a,n)=1$. Recall that every entry of $\Delta'=(\Delta'_{i,j})$ carries exactly one factor of

$$P_n(a)=\frac{n-1}{2}\prod_{\substack{1\le i<n\\ \gcd(i,n)=1}}\Big(\frac{a^i-1}{a-1}-i+\tfrac{n-1}{2}\Big)\Big(\frac{a^{n-1}-a^i}{a-1}+i-\tfrac{n-1}{2}\Big)\,(a^i-1).$$

Define the matrix

$$M(a) \;=\; \frac{1}{P_n(a)}\,\Delta',$$

so that

$$\det\Delta' = P_n(a)^n\,\det M(a), \qquad \big|\Delta'^0_0\big| = P_n(a)^{\,n-1}\,\big|M_0{}^0(a)\big|.$$

Hence the ratio of interest is

$$\frac{P_n(a)\,\big|\Delta'^0_0\big|}{\big|\Delta'\big|} \;=\; \frac{\big|M_0{}^0(a)\big|}{\det M(a)} \;=: F(a).$$

Step 1 (Constancy). Both $\det M(a)$ and $\big|M_0{}^0(a)\big|$ lie in $\mathbb{Z}[a,a^{-1}]$ and have the same total degree in a. Therefore their quotient

$$F(a)=\frac{\big|M_0{}^0(a)\big|}{\det M(a)}$$

is a Laurent polynomial of degree zero with integer coefficients, hence a constant integer C independent of a.

Step 2 (Asymptotics as $a\to\infty$). We compute

$$C=\lim_{a\to\infty}F(a).$$

From the definitions one checks:

$$M_{0,0}(a)=\sum_{\substack{1\le i<n\\ \gcd(i,n)=1}}\frac{a^{k(i)}}{\frac{a^i-1}{a-1}-i+\frac{n-1}{2}}=\frac{2}{n-1}+O\big(a^{-1}\big),$$

$$M_{1,1}(a)=\frac{2\big(a^{\varphi(n)-1}+1\big)}{n-1}+\frac{1}{a-1}=\frac{2}{n-1}\,a^{\varphi(n)-1}+O\big(a^{\varphi(n)-2}\big),$$

$$M_{i,i}(a)=O\big(a^{\varphi(n)-2}\big)\quad(i\ge 2),\qquad M_{i,j}(a)=O\big(a^{-1}\big)\quad(i\ne j).$$

In the Leibniz expansions of $\det M(a)$ and of the minor $\left|{M_0}^0(a)\right|$, the unique permutation of maximal total a–degree is the identity. Hence

$$\begin{aligned}\det M(a) &= \big(M_{0,0}(a)\, M_{1,1}(a) \prod_{i=2}^{n-1} M_{i,i}(a)\big) + O\big(a^{(\varphi(n)-1)+(n-1)(\varphi(n)-2)-1}\big)\\ &= \frac{4}{(n-1)^2}\, a^{\varphi(n)-1} \;+\; o\big(a^{\varphi(n)-1}\big),\\ \left|{M_0}^0(a)\right| &= M_{1,1}(a) \prod_{i=2}^{n-1} M_{i,i}(a) \;+\; o\big(a^{\varphi(n)-1}\big) = \frac{2}{n-1}\, a^{\varphi(n)-1} \;+\; o\big(a^{\varphi(n)-1}\big).\end{aligned}$$

Observe that for all $i \neq j$ one has

$$M_{i,j}(a) \;=\; O\big(a^{\varphi(n)-2}\big),$$

whereas each diagonal entry satisfies

$$M_{i,i}(a) = \frac{2}{n-1}\, a^{\varphi(n)-1} + O\big(a^{\varphi(n)-2}\big).$$

In the Leibniz expansion $\det M(a) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=0}^{n-1} M_{i,\sigma(i)}(a)$, any term corresponding to a non-identity permutation $\sigma \neq \mathrm{id}$ contains at least one off-diagonal factor $M_{i,\sigma(i)}(a)$ and hence is

$$O\Big(a^{(n-2)(\varphi(n)-1)+(\varphi(n)-2)}\Big) \;=\; o\big(a^{(n-1)(\varphi(n)-1)}\big).$$

Consequently the unique contribution of maximal total a–degree $(n-1)(\varphi(n)-1)$ comes from the identity permutation, yielding

$$\det M(a) = \prod_{i=0}^{n-1} M_{i,i}(a) + o\big(a^{(n-1)(\varphi(n)-1)}\big) = \frac{4}{(n-1)^2}\, a^{(n-1)(\varphi(n)-1)} + o\big(a^{(n-1)(\varphi(n)-1)}\big),$$

which justifies taking the limit $a \to \infty$.

Therefore

$$F(a) = \frac{\left|{M_0}^0(a)\right|}{\det M(a)} = \frac{\dfrac{2}{n-1}\, a^{\varphi(n)-1} + o(a^{\varphi(n)-1})}{\dfrac{4}{(n-1)^2}\, a^{\varphi(n)-1} + o(a^{\varphi(n)-1})} \longrightarrow \frac{n-1}{2}.$$

Since $F(a) \equiv C$ is constant, it follows $C = (n-1)/2$. Finally, we have

$$\frac{n-1}{2} \equiv 1 \pmod{n}$$

Since $0 < 2z < n$ and $2z|n-1$ and n is odd prime-power-free, the only solution of $x \equiv 1 \pmod{n}$ with $0 < x < n$ is $x = n-1$ so

$$2z = n-1, \quad \text{i.e.} \quad z = \frac{n-1}{2}.$$

Therefore

$$z = \frac{n-1}{2} \quad \text{implies} \quad \frac{n-1}{\varphi(n)} \equiv \frac{n-1}{2} \pmod{n}.$$

Suppose for contradiction that $n > 1$ is composite, $\varphi(n) \mid (n-1)$, and

$$\frac{n-1}{\varphi(n)} \equiv \frac{n-1}{2} \pmod{n}.$$

Since $\varphi(n) \mid (n-1)$, we may write

$$k = \frac{n-1}{\varphi(n)},$$

where k is a positive integer. The congruence then says there exists an integer t such that

$$k = \frac{n-1}{2} + t\,n.$$

On the other hand, for any composite $n > 2$ we have

$$1 < \varphi(n) \leq n-2 \quad \Longrightarrow \quad 1 < \frac{n-1}{\varphi(n)} < \frac{n-1}{1} = n-1,$$

i.e. $1 < k < n-1$. Meanwhile

$$0 < \frac{n-1}{2} < n,$$

so the only way

$$k = \frac{n-1}{2} + t\,n \quad \text{with} \quad 1 < k < n-1$$

is to have $t = 0$. Hence

$$k = \frac{n-1}{2} \quad \Longrightarrow \quad \frac{n-1}{\varphi(n)} = \frac{n-1}{2} \quad \Longrightarrow \quad \varphi(n) = 2.$$

But $\varphi(n) = 2$ forces $n = 3$ or $n = 4$. The case $n = 3$ is prime, and $n = 4$ gives $\varphi(4) = 2 \nmid 3$. Thus no composite n can satisfy the given congruence. Therefore, no composite counterexample $n > 6$ exists that resolves the Lehmer totient problem.

□

□

Example: Leibniz expansion for $n = 9$

Here we illustrate the "highest-degree" argument in the composite case $n = 9$, where $\varphi(9) = 6$.

1. **Setup.** After clearing denominators in the Laplacian minor one obtains a 9×9 matrix $M(a) = (M_{i,j}(a))$ with asymptotics as $a \to \infty$:

   $$M_{0,0}(a) = \frac{1}{4} + O\big(a^{-1}\big), \quad M_{1,1}(a) = \frac{1}{4}\, a^5 + O\big(a^4\big), \quad M_{i,i}(a) = O\big(a^4\big) \ (i = 2, \ldots, 8),$$

   and every off-diagonal entry satisfies $M_{i,j}(a) = O(a^4)$ for $i \neq j$.

2. **Determinant expansion.** By the Leibniz formula

   $$\det M(a) = \sum_{\sigma \in S_9} \operatorname{sgn}(\sigma) \prod_{i=0}^{8} M_{i,\sigma(i)}(a).$$

   The *identity* permutation contributes total degree

   $$\deg(M_{0,0}) + \deg(M_{1,1}) + \sum_{i=2}^{8} \deg(M_{i,i}) = 0 + 5 + 7 \cdot 4 = 33.$$

   Any other permutation uses at least one entry of degree ≤ 4 in place of either $M_{0,0}$ or $M_{1,1}$, giving total degree $\leq 29 < 33$. Hence the identity term is the unique top-degree contributor.

3. **Leading-coefficient calculation.** Extracting the coefficient of a^{33} from the identity term yields

   $$\left(\tfrac{1}{4}\right) \times \left(\tfrac{1}{4}\right) \times \left(\tfrac{1}{4}\right)^7 = (1/4)^9.$$

   Thus

   $$\det M(a) \;=\; (1/4)^9\, a^{33} \;+\; \big(\text{lower-degree terms}\big).$$

4. **Subminor and the ratio.** Let $M_{00}(a)$ be the (8×8) minor deleting row 0 and column 0. An identical degree-count shows

   $$\det M_{00}(a) = (1/4)^8\, a^{33} + \big(\text{lower-degree terms}\big).$$

   Therefore

   $$F(a) \;=\; \frac{\det M_{00}(a)}{\det M(a)} \;\xrightarrow[a \to \infty]{}\; \frac{(1/4)^8}{(1/4)^9} \;=\; 4 \;=\; \frac{9-1}{2}.$$

This confirms that, in the composite case $n = 9$, the unique highest-degree term in each minor comes from the identity permutation, and forces $\lim_{a \to \infty} F(a) = (n-1)/2 = 4$.

References

[1] B. C. Kellner and M. Schmitt, *A Survey of the Lehmer Totient Problem*, Integers **11A** (2011), Article A11.

[2] P. G. Doyle and J. L. Snell, *Random Walks and Electric Networks*, Mathematical Association of America, 1984.

[3] G. Strang, *Linear Algebra and Its Applications*, 4th ed., Brooks–Cole, 2005.

[4] N. Biggs, *Algebraic Graph Theory*, 2nd ed., Cambridge University Press, 1997.

[5] S. Lang, *Algebra*, 3rd ed., Addison–Wesley, 1993.

[6] F. R. K. Chung, *Spectral Graph Theory*, CBMS Regional Conference Series in Mathematics No. 92, 1997.