The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

A Ring-theoretic Approach to Bound the Totient Function

B. Sury

To cite this article: B. Sury (2019) A Ring-theoretic Approach to Bound the Totient Function, The American Mathematical Monthly, 126:2, 167-167, DOI: 10.1080/00029890.2019.1537458

To link to this article: https://doi.org/10.1080/00029890.2019.1537458

Published online: 11 Feb 2019.

Department of Statistics, Università "Luigi Bocconi," via Roentgen 1, 20136 Milan, Italy
leonetti.paolo@gmail.com

A Ring-theoretic Approach to Bound the Totient Function

Let A be a possibly noncommutative ring with unity and let A^* denote its group of units. We show the following.

Proposition. *(i) If A is infinite, and not a division ring, then $A \setminus A^*$ is infinite.*
(ii) If A is finite, and not a division ring, then $|A| \leq (|A| - |A|^*)^2$.
In particular, for $n > 1$, $\phi(n) \leq n - \sqrt{n}$ if and only if n is not a prime.

Proof. To prove (i), assume A is infinite, and $A \setminus A^*$ is finite. Then any left ideal $I \neq A$ satisfies $I \cap A^* = \emptyset$; so, I is finite. Consider any $a \in A \setminus A^*$ such that $a \neq 0$. Since A is not a division ring, either $1 \notin Aa$ or $1 \notin aA$. If $Aa \neq A$, then the left ideals Aa and $I_a := \{b \in A : ba = 0\}$ are proper left ideals. This means both are finite. But, A/I_a is in bijection with Aa which means A is finite, which is a contradiction of our assumption. Therefore, (i) is proved if $Aa \neq A$. Similarly, if $aA \neq A$, one may work with the right ideals aA and $\{b \in A : ab = 0\}$ and arrive at a contradiction.

To prove (ii) when A is finite, consider any left ideal $I \neq A$. As $I \cap A^* = \emptyset$, we have $|I| \leq |A| - |A^*|$ as before. Let $a \in A \setminus A^*$ be such that $a \neq 0$. Since A is not a division ring, either $Aa \neq A$ or $aA \neq A$. If $Aa \neq A$, the left ideals Aa and $I_a = \{b \in A : ba = 0\}$ are proper; hence $|Aa|$ and $|I_a|$ are both at most $|A| - |A^*|$. But, A/I_a is in bijection with Aa and so, $|A| \leq (|A| - |A^*|)^2$. In the case $aA \neq A$, the proof is similar. Note that if $A = \mathbb{Z}/n\mathbb{Z}$ for some $n > 1$, then we know that A is a division ring if and only if it is a field, which happens if and only if n is prime. Thus, for $n > 1$ composite, we have $n \leq (n - \phi(n))^2$; hence, $\phi(n) \leq n - \sqrt{n}$. ∎

—Submitted by B. Sury,
Statistics & Mathematics Unit, Indian Statistical Institute

doi.org/10.1080/00029890.2019.1537458
MSC: Primary 12F15, Secondary 11F25