98.03 Explicit solutions of $\phi(m) = k!$

In [1] Peter Shiu considered the equations $\phi(m) = k!$ and $\sigma(n) = k!$. He discusses interesting algorithms for each of these equations. For several years (at least since 1995), I had known a way of getting an explicit solution for the former which I have been sharing with mathematics olympiad students. The paper [2] not only mentions this method but goes on to prove that there are infinitely many common values of the ϕ and the σ functions. Since Shiu comments in [1] that it is unknown whether the ranges of the totient function and the 'sum of divisors' function have infinite intersection, I thought it would be a good idea to draw attention to [2] and also recall my simple explicit solution for the readers of the *Gazette*.

We recall just one definition. For a positive integer $n > 1$ with the prime decomposition $n = \prod_{i=1}^{r} p_i^{a_i}$, the *radical* of n, denoted by $\mathrm{rad}(n)$, is the product $\prod_{i=1}^{r} p_i$; it is the largest square-free divisor of n.

Theorem: Let $n = \prod_{i=1}^{r} p_i^{a_i} > 1$ be a positive integer. If $\phi(\mathrm{rad}(n))$ divides n, then $\phi(n)$ divides n^2 and

$$\phi\left(\frac{n^2}{\phi(n)}\right) = n.$$

Further, $\frac{n^2}{\phi(n)}$ is the unique solution in this case which shares the same prime divisors with n.*

As we shall see, each $n = k!$ satisfies the hypothesis of the theorem; that is, we claim that $\phi(\mathrm{rad}(k!))$ divides $k!$, so that we have the following result.

Corollary: For any positive integer k, $\phi(k!)$ divides $(k!)^2$, and

$$\phi\left(\frac{(k!)^2}{\phi(k!)}\right) = k!.$$

Further, the positive integer $\frac{(k!)^2}{\phi(k!)}$ is the unique solution which shares the same prime divisors with $k!$.

Proof of the corollary: We claim that $\phi(\mathrm{rad}(k!))$ divides $k!$, so that the theorem will apply to yield the corollary. To prove the claim, first note that a prime number p divides $k!$ if, and only if, $p \leqslant k$. So, if $p_1 < p_2 < \ldots < p_r$ are the entirety of prime numbers not exceeding k, then we may write

$$k! = \prod_{i=1}^{r} p_i^{a_i}.$$

* Please clarify the meaning of this sentence.

Also, the positive integer $\text{rad}(k!) = \prod_{i=1}^{r} p_i$ satisfies the property that $\phi(\text{rad}(k!)) = \prod_{i=1}^{r} p_i$ divides $k!$ since *each* $p_i - 1$ *occurs as a distinct term* in $k! = k(k-1)(k-2)\ldots 2 \times 1$.

This proves the claim. Hence the corollary follows from the theorem.

Proof of the theorem: As $\phi(\text{rad}(n)) = \prod_{i=1}^{r}(p_i - 1)$ is assumed to divide $n = \prod_{i=1}^{r} p_i^{a_i}$, we may write

$$\phi(\text{rad}(n)) = \prod_{i=1}^{r}(p_i - 1) = \prod_{i=1}^{r} p_i^{b_i}$$

with $0 \leqslant b_i \leqslant a_i$.

Then we have

$$\frac{n^2}{\phi(n)} = \prod_{i=1}^{r} \frac{p_i^{2a_i}}{p_i^{a_i - 1}(p_i - 1)} = \prod_{i=1}^{r} p_i^{a_i - b_i + 1},$$

which is an integer. Thus, $\phi(n)$ divides n^2.

Further, we have

$$\phi\left(\frac{n^2}{\phi(n)}\right) = \prod_{i=1}^{r} \phi\left(p_i^{a_i - b_i + 1}\right) = \prod_{i=1}^{r} p^{a_i - b_i}(p_i - 1) = \prod_{i=1}^{r} p^{a_i} = n.$$

Also, if $\phi(\text{rad}(n))$ divides n, then evidently both $\frac{n^2}{\phi(n)}$ and n have the same prime factors $p_1, \ldots, p_r$.

Conversely, if $m = \prod_{i=1}^{r} p_i^{c_i}$ has the same prime factors as n (so $c_i > 0$ for all i), then

$$\frac{m}{\phi(m)} = \prod_{i=1}^{r} \frac{1}{1 - 1/p_i} = \frac{n}{\phi(n)}.$$

Hence, if $\phi(m) = n$, then we have $m = \frac{n^2}{\phi(n)}$.

This completes the proof.

Remark: We comment very briefly on the proof of the corollary. Note that, if $p_1, \ldots, p_r$ are primes dividing a certain number n such that each $p_i - 1$ divides n as well, then, in general, some conditions on n are required if we are to assert truthfully that the product $\prod_{i=1}^{r}(p_i - 1)$ divides n. The special nature of a number n of the form $k!$ is what makes the proof work.

For example, look at $n = 18!$. The primes dividing 18! are all the primes less than 18, that is, 2, 3, 5, 7, 11, 13, 17. Now, the product

$$(2-1)(3-1)(5-1)(7-1)(11-1)(13-1)(17-1) = 1.2.4.6.10.12.16$$

divides 18! because each factor appears in

$$18! = 18.17.16.15.14.13.12.11.10.9.8.7.6.5.4.3.2.1.$$

Acknowledgment: The author would like to thank an anonymous referee and the editor for their input which made the proofs more transparent; in particular, they suggested including an example, as in the above remark.

References

1. Peter Shiu, Solutions to $\phi(m) = k!$ and $\sigma(n) = k!$, *Math. Gaz.* **97** (March 2013) pp. 110-115.
2. Kevin Ford, Florian Luca, and Carl Pomerance, Common values of the arithmetic functions, *Bull. London Math. Soc*., Vol. **42** (2010) pp. 478-488.

B. SURY

Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India

e-mail: *sury@isibang.ac.in*