

10966. Proposed by Jean-Marie De Koninck, Université Laval, Québec, Canada.

(a) Let ϕ denote the Euler ϕ function, and let $\gamma(n) = \prod_{p|n} p$, with $\gamma(1) = 1$. Prove that there are exactly six positive integers such that $\phi(n) = (\gamma(n))^2$.

(b)* Let $\sigma(n)$ denote the sum of divisors of n . Prove or disprove that the only solutions to $\sigma(n) = (\gamma(n))^2$ are $n = 1$ and $n = 1782$.

Solution: The first result will follow from a more general theorem, which will be proved. This theorem includes an algorithm whose output proves (a). There will also be an outline of a possible resolution of (b); some partial results will be presented.

Theorem. For any integer $k > 0$, there are a finite number of integers n such that $\phi(n) = \gamma(n)^k$. Furthermore, there is a “sophisticated” algorithm to find all such n .

Proof of the theorem: Write $\gamma = \gamma(n)$ and $\phi = \phi(n)$, and suppose $\gamma^k = \phi$. Write n as a product of prime numbers:

$$n = \prod_{i=1}^L p_i^{\alpha_i}, \quad \text{so that } \gamma = \prod_{i=1}^L p_i \quad \text{and} \quad \phi = \prod_{i=1}^L (p_i - 1)p_i^{\alpha_i - 1},$$

where $p_1 < p_2 < \dots < p_L$, and $\alpha_i > 0$, for all applicable i . The finiteness result will follow after three claims are proven:

(1) $\alpha_i \leq k + 1$, for all $i = 1, 2, \dots, L$.

If $\phi = \gamma^k$, then equating the above formulas for γ and ϕ implies that

$$\prod_{i=1}^L (p_i - 1) = \phi \prod_{i=1}^L p_i^{1 - \alpha_i} = \gamma^k \prod_{i=1}^L p_i^{1 - \alpha_i} = \prod_{i=1}^L p_i^{k + 1 - \alpha_i}. \quad (\text{E1})$$

Since the left-hand side is an integer, the right-hand side must also be one. Hence $k + 1 - \alpha_i \geq 0$, which proves (1).

(2) $L \leq k + 1$.

First, $p_1 = 2$; this can be shown with (E1): if n is odd, then the left-hand side of (E1) is even, and the right-hand side is odd. Now we look for the highest power of 2 which divides into both sides. That power is at least L on the left-hand side, and on the right-hand side it is $k + 1 - \alpha_1 \leq k + 1$. This proves (2).

(3) $p_L \leq Q_k(L) \leq Q_k(k + 1)$, where $Q_k(h)$ is the function defined by

$$Q_k(h) = \begin{cases} 2, & \text{if } i = 1; \\ 1 + Q_k(1)^k Q_k(2)^k \dots Q_k(i - 1)^k, & \text{otherwise.} \end{cases}$$

The second inequality in the statement of (3) follows because Q_k is an increasing function.

To prove the first inequality is true, we will show $R(i)$ is true for $j = L$, where $R(i)$ denotes the proposition

“For all $1 \leq i \leq j$, $p_i \leq Q_k(h)$, and there exist j integers $\beta_1, \beta_2, \dots, \beta_j$ between 0 and $k + 1$ such that

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_j^{\beta_j} \cdot p_{j+1}^{k+1-\alpha_{j+1}} p_{j+2}^{k+1-\alpha_{j+2}} \dots p_L^{k+1-\alpha_L} = \prod_{i=j+1}^L (p_i - 1).” \quad (\text{E2})$$

This will be proven by induction on j . The proposition $R(1)$ is true because $p_1 = 2$, and the equality (E2) is the equality (E1) above when $j = 1$.

Now suppose $R(j)$ is true, and consider the prime factors of $p_{j+1} - 1$. Since $p_{j+1} - 1$ is strictly less than p_{j+1}, \dots, p_L , the only possible prime factors of $p_{j+1} - 1$ are among p_1, p_2, \dots, p_j .

(Otherwise some prime divides evenly into the right-hand side of (E2) but not the left-hand side.) So we may write

$$p_{j+1} - 1 = p_1^{\delta_1} p_2^{\delta_2} \cdots p_j^{\delta_j},$$

for some $\delta_1, \delta_2, \dots, \delta_j$.

The highest power of p_i that divides evenly into the left-hand side of (E2) is β_i (if $i \leq j$), so $0 \leq \delta_i \leq \beta_i$, for all $i \leq j$. Thus

$$\begin{aligned} p_{j+1} &= 1 + p_1^{\delta_1} p_2^{\delta_2} \cdots p_j^{\delta_j} \leq p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j} \\ &\leq p_1^{k+1} p_2^{k+1} \cdots p_j^{k+1} \leq 1 + Q_k(1)^k Q_k(2)^k \cdots Q_k(j)^k = Q_k(j+1). \end{aligned}$$

To prove (E2) for $j+1$, note that

$$\begin{aligned} \prod_{i=j+2}^L (p_i - 1) &= \frac{\prod_{i=j+1}^L (p_i - 1)}{p_{j+1} - 1} \\ &= \frac{p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j} \cdot p_{j+1}^{k+1-\alpha_{j+1}} p_{j+2}^{k+1-\alpha_{j+2}} \cdots p_L^{k+1-\alpha_L}}{p_1^{\delta_1} p_2^{\delta_2} \cdots p_j^{\delta_j}} \\ &= p_1^{\beta_1-\delta_1} p_2^{\beta_2-\delta_2} \cdots p_j^{\beta_j-\delta_j} \cdot p_{j+1}^{k+1-\alpha_{j+1}} p_{j+2}^{k+1-\alpha_{j+2}} \cdots p_L^{k+1-\alpha_L}, \end{aligned}$$

so $R(j+1)$ is true, if $R(j)$ is. This proves claim (3).

Putting claims (1), (2), and (3) together, we get

$$n = \prod_{i=1}^L p_i^{\alpha_i} \leq \prod_{i=1}^L p_i^{k+1} \leq \prod_{i=1}^L Q_k(k+1)^{k+1} \leq [Q_k(k+1)^{k+1}]^L \leq [Q_k(k+1)]^{(k+1)^2},$$

which shows that there are only a finite number of integers n such that $\phi = \gamma^k$.

Now for the algorithm. A “non-sophisticated” algorithm exists to determine all values of n such that $\phi = \gamma^k$, namely the one which checks all integers between 1 and $[Q_k(k+1)]^{(k+1)^2}$. A more “sophisticated” one exists, which does not require (nearly) as much time. This algorithm proceeds along the line of the proof, and proceeds in two phases. Quantities in brackets should be read as arrays (ordered lists).

- (I) Put $(j, 1, [k+1], [2])$ on a “stack” (a queue also works), for all j between 1 and $k+1$.
- (II) While there is an item $(L, j, [\beta_1, \beta_2, \dots, \beta_j], [p_1, p_2, \dots, p_j])$ on the stack, do the following: If $j = L$, then output the factorization $p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}$ (as a value of n where $\phi(n) = \gamma(n)^k$). Otherwise, find all sequences $[\delta_1, \delta_2, \dots, \delta_j]$ such that

- (a) $\beta_i - 1 \geq \delta_i \geq 0$, for $i = 1, 2, \dots, j$; and
- (b) $P = 1 + p_1^{\delta_1} p_2^{\delta_2} \cdots p_j^{\delta_j}$ is prime and greater than p_j ;

and put the item $(L, j+1, [\beta_1 - \delta_1, \beta_2 - \delta_2, \dots, \beta_j - \delta_j, k+1], [p_1, p_2, \dots, p_j, P])$ on the stack.

Note that the item $(L, j, [\beta_1, \beta_2, \dots, \beta_j], [p_1, p_2, \dots, p_j])$ being on the stack means that (E2) is true.

This proves the theorem. ■

Using the algorithm given in the theorem for $k = 2$ produces the numbers 1 (where $L = 0$), 2^3 ($L = 1$), $2^2 \cdot 3^3$ and $2^1 \cdot 5^3$ ($L = 2$), and $2 \cdot 3^2 \cdot 7^3$ and $2 \cdot 3^1 \cdot 19^3$ ($L = 3$). (The bound given by the theorem (101^9) is many orders of magnitude larger than the actual upper bound (43,434), but this is typical of finiteness results.)

Turning to part (b), a similar approach was attempted, and some partial results have been obtained. Using the prime factorization of n , we have $\sigma = \sigma(n) = S_1 S_2 \cdots S_L$, where $S_i = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$. The goal then is to find the prime factorization of S_i , for all i , assuming that $\sigma n = \gamma(n)^2$. This means that the prime factors of S_i are among p_1, p_2, \dots, p_L . Also, no cube of p_j divides into S_i , so this suggests a combinatorial (“finite”) approach may also work here.

Partial results are given below as a list of lemmas.

Lemma 1. *Suppose $\sigma = \gamma^2$, and $n > 1$. Then:*

- (a) *There is an I such that $\alpha_I = 1$;*
- (b) *$p_1 = 2$;*
- (c) *$p_i \nmid S_i$;*
- (d) *$p_j \nmid S_I$, if $j > I$;*
- (e) *If $p_1 \nmid S_i$, then α_i is even, for any $i > 1$;*
- (f) *If $p_1 \mid S_i$, then $\alpha_i \equiv 1 \pmod{4}$, for any i ;*
- (g) *If $i = \max\{j : p_1 \mid S_j\}$, then $\alpha_i = 1$.*
- (h) *$S_i \neq 1$, and if $S_i = p_j$, then $p_i < p_j$ (and hence $i < j$);*
- (i) *If $S_j = p_i^2$ and $i < j$, then $(i, j) = (1, 2)$, $p_2 = 3$, and $\alpha_2 = 1$.*

Proof: If $\alpha_i \geq 2$ for all i , then $S_i \geq 1 + p_i + p_i^2 > p_i^2$, and thus

$$\sigma = \prod_{i=1}^L S_i > \prod_{i=1}^L p_i^2 = \gamma^2.$$

This proves (a).

To prove (b), suppose that every p_i is odd. Part (a) implies that

$$\prod_{i=1}^L p_i^{\beta_i} = S_I = 1 + p_I,$$

for some nonnegative integers β_1, \dots, β_L . But the left-hand side is the product of odd numbers and is hence odd; the right-hand side is even. This contradiction proves (b).

Part (c) follows because $S_i \equiv 1 \pmod{p_i}$ (since $p_i^j \equiv 0 \pmod{p_i}$, for all i and j).

Part (d) follows because otherwise

$$p_j \leq \prod_{i=1}^L p_i^{\beta_i} = S_I = 1 + p_I < 1 + (p_j - 1) = p_j,$$

where β_i are nonnegative integers and $\beta_j \geq 1$.

To prove (e), suppose $p_1 \nmid S_i$. Then S_1 is odd, and since $i > 1$, $p_i > 2$, and p_i is odd as well. Thus,

$$1 \equiv S_i \equiv 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} \equiv 1 + 1 + \cdots + 1 \equiv \alpha_i + 1 \pmod{2},$$

which proves (e). A similar equality shows that if $p_1 \mid S_i$, then α_i is odd, which proves part of (f). Now, if $\alpha_i = 4m + 3$ for some integer m , then

$$S_i = 1 + p_i + p_i^2 + \cdots + p_i^{4m+3} = (1 + p_i) \cdot \left(1 + p_i^2 + p_i^4 \cdots + p_i^{2(2m+1)}\right),$$

which implies that $p_1^2 \mid S_i$ (because $1 + p_i^2 + p_i^4 \cdots + p_i^{2(2m+1)}$ is even). Thus, for every $j \neq i$, $p_1 \nmid S_j$, and hence $\alpha_j \geq 2$, by (e). By hypothesis, $\alpha_i \geq 3$; but then these inequalities violate (a). This proves (f).

If (g) does not hold, then $\alpha_i \geq 5$, by (f). If $p_1^2 \mid S_i$, then

$$S_k > \begin{cases} p_k^4 > p_k^2 \cdot p_1, & \text{if } k = i; \\ p_k, & \text{if } k = 1; \\ p_k^2, & \text{if } k \neq 1, i, \text{ since } \alpha_k \text{ is even.} \end{cases}$$

Multiplying these inequalities together for all k results in the inequality $\sigma > \gamma^2$.

If $p_1 \mid S_j$, where $j < i$, then

$$S_k > \begin{cases} p_k^5 > p_k^2 \cdot p_1 \cdot p_j, & \text{if } k = i; \\ p_k, & \text{if } k = j; \\ p_1, & \text{if } k = 1; \\ p_k^2, & \text{if } k \neq 1, i, j. \end{cases}$$

Once again, multiplying these inequalities together yields $\sigma > \gamma^2$. This proves (g).

If (h) does not hold, then $1 + p_j < 1 + p_i = S_i = p_j$.

Finally, we show (i): Note that $p_j^{\alpha_j} < S_j = p_i^2 < p_j^2$, so $1 \leq \alpha_j < 2$. Hence $\alpha_j = 1$, which implies that $p_1 \mid S_j$ by (e). Hence $1 + p_j = S_j = p_1^2 = 4$, or $p_j = 3$. But then we must have $j = 2$ as well, since $p_3 \geq 5$. ■

Now for the constructive results:

Lemma 2. *If $L = 1$ or 2 , then $\sigma(n) \neq \gamma(n)^2$ (where L and α_* come from the prime factorization of n).*

Proof: If $L = 1$, then Lemma 1(a) and (b) imply that $n = 2^1$, but $\sigma(2) = 3 \neq 2^2$.

If $L = 2$, then Lemma 1(c) implies that $p_1^2 = S_2$ and $p_2^2 = S_1$. Lemma 1(g) implies that $\alpha_2 = 1$, so $4 = p_1^2 = S_2 = 1 + p_2$, so $p_2 = 3$. This implies that $9 = p_2^2 = S_1 = 1 + p_1 + \dots + p_1^{\alpha_1}$, but there is no integer α_1 which makes this equality true. Hence there are no values of n where $\sigma = \gamma^2$, if $L = 2$. ■

Lemma 3. *If $L = 3$ and $\sigma = \gamma^2$, then $n = 1782 = 2 \cdot 3^4 \cdot 11$.*

Proof: The general method of proof will be determining which of the prime factors p_1 , p_2 , and p_3 divide evenly into each of S_1 , S_2 , and S_3 and whether p_1^2 , p_2^2 , or p_3^2 divides evenly into any of them. There are only a finite number of ways for this to happen, since there are only six prime factors and three values of S_i ($p_1^2 p_2^2 p_3^2 = S_1 S_2 S_3$)—one possibility is that $S_1 = p_2$, $S_2 = p_3^2$, and $S_3 = p_1^2 p_2$. Then some bounds will be determined for α_i from these equations; it turns out that certain exponents cannot be too large without a contradiction occurring—in the example given, it is shown that α_2 is 2 or 4, because the assumption that $\alpha_2 \geq 6$ lead to contradictions. Finally, the information about some α_i will be used to find out further information about the values of the other S_i 's, and the primes p_i ; most of the time, this new information will lead to a quick contradiction. In the example given, it is shown if $\alpha_2 = 4$, then $p_2 = 3$, $\alpha_1 = 1$, $S_2 = 121$, $p_3 = 11$, and $n = 1782$ (which are deduced in this order); if $\alpha_2 = 2$, then a contradiction results (p_3 must be $3/5$ or 0 , neither of which is a prime number). It is likely that using this technique, the conjecture may be resolved for values of n with $L > 3$.

Now suppose $\sigma = \gamma^2$. Note that $p_1 \mid S_3$, because otherwise, $S_3 = p_2$ or $S_3 = p_2^2$, which do not happen, according to Lemma 1(h) and (i). Also because of Lemma 1(h) and (i), $S_3 \neq p_1, p_1^2$, so $S_3 = p_1^2 p_2^2$ (Case I), $S_3 = p_1 p_2^2$ (Case II), $S_3 = p_1 p_2$ (Case III), or $S_3 = p_1^2 p_2$ (Case IV). Furthermore, $\alpha_3 = 1$, by Lemma 1(g).

We eliminate Case I first; if $S_3 = p_1^2 p_2^2$,

$$p_3 = S_3 - 1 = p_1^2 p_2^2 - 1 = (p_1 p_2 - 1)(p_1 p_2 + 1),$$

which is a non-trivial factorization of p_3 , as $p_1 p_2 - 1 \geq 2 \cdot 3 - 1 > 1$.

Now for Case II. Since $p_1^2 \nmid S_3$, $p_1 \mid S_2$; otherwise $p_1 \mid S_1$, contradicting Lemma 1(c). Since $S_2 \neq p_1$, $p_3 \mid S_2$ as well, because of Lemma 1(h). If $p_3^2 \mid S_2$, then, in order for σ to equal γ^2 , we must have $S_1 = 1$, which contradicts Lemma 1(h). Thus $p_3 \mid S_1$, and we have $S_1 = p_3$ and $S_2 = p_1 p_3$; in particular,

$$p_3 = S_1 = 1 + 2 + \dots + 2^{\alpha_1} = 2^{\alpha_1 + 1} - 1, \quad \text{and so}$$

$$2p_2^2 = p_1 p_2^2 = S_3 = 1 + p_3 = 2^{\alpha_1 + 1},$$

but then p_2 divides evenly into the left-hand side and not into the right-hand side. This takes care of Case II.

Now consider Case III ($S_3 = p_1^2 p_2$, noting that $p_3 = 4p_2 - 1$). Since $S_1 S_2 S_3 = p_1^2 p_2^2 p_3^2$ and $p_2 \nmid S_2$, $p_2 \mid S_1$. Similarly, $p_3 \mid S_2$. Thus we either have $S_2 = p_3^2$ and $S_1 = p_2$ (Case IIIA) or $S_2 = p_3$ and $S_1 = p_2 p_3$ (Case IIIB).

For Case IIIA: $S_2 = p_3^2 = (4p_2 - 1)^2$, and α_2 is even. If $\alpha_2 \geq 4$, then

$$(4p_2 - 1)^2 = p_3^2 = S_2 \geq p_2^4 \quad [> 0],$$

so $4p_2 - 1 \geq p_2^2$, which implies that $p_2 = 3$, and consequently $p_3 = S_3 - 1 = 4p_2 - 1 = 11$. We also have $\alpha_2 = 4$, because if $\alpha_2 \geq 6$,

$$121 = 11^2 = (4p_2 - 1)^2 = S_2 > p_2^6 = 3^6 = 729.$$

Since

$$2^{\alpha_1+1} - 1 = 1 + p_1 + \cdots + p_1^{\alpha_1} = S_1 = p_2 = 3,$$

$\alpha_1 = 1$. Thus $n = 2^1 \cdot 3^4 \cdot 11^1 = 1782$.

If $\alpha_2 = 2$, then

$$(4p_2 - 1)^2 = p_3^2 = S_2 = 1 + p_2 + p_2^2,$$

which implies that $p_2 = 3/5$ or 0 , neither of which is prime. This settles Case IIIA.

For Case IIIB: $S_2 = p_3$ has no p_1 factors, so by Lemma 1(e), α_2 is even and at least two. Hence

$$1 + p_2 + p_2^2 \leq S_2 = p_3 = 4p_2 - 1,$$

which implies that $p_2^2 - 3p_2 + 2 \leq 0$, which only occurs if $1 \leq p_2 \leq 2$. Since $p_2 > p_1 = 2$, this is a contradiction. This takes care of Case III.

Now we turn to Case IV, where $S_3 = p_1 p_2$ and hence $p_3 = 2p_2 - 1$. Because there needs to be another p_1 factor and another p_2 factor in $S_1 S_2 S_3$, $p_1 \mid S_2$ and $p_2 \mid S_1$. Since $p_3 \nmid S_3$, we must have $S_2 = p_1$ (which cannot occur, by Lemma 1(h)), $S_2 = p_1 p_3$ (Case IVA), or $S_2 = p_1 p_3^2$ (Case IVB).

We consider Case IVA: If $\alpha_2 \geq 5$, then

$$2(2p_2 - 1) = p_1 p_3 = S_2 > 1 + p_2^2 + p_2^5 > p_2^2 + 2, \quad \text{or}$$

$$0 > p_2^2 - 4p_2 + 4 = (p_2 - 2)^2.$$

Thus, $\alpha_2 \not\geq 5$, and so by Lemma 1(f), $\alpha_2 = 1$, and

$$1 + p_2 = S_2 = 2(2p_2 - 1) = 4p_2 - 2,$$

which implies that $p_2 = 1$. This is not possible, either.

Finally, consider Case IVB. If $\alpha_2 \geq 5$, then

$$8p_2^2 - 8p_2 + 2 = 2(2p_2 - 1)^2 = p_1 p_3^2 = S_2 > 1 + p_2 + p_2^5 > 1 + 1 + 2p_2^3 = 2 + 2p_2^3,$$

which implies that $8p_2^2 - 8p_2 > 2p_2^3$, or

$$0 > 2p_2^2 - 8p_2 + 8 = 2(p_2 - 2)^2.$$

Thus $\alpha_2 = 1$ by Lemma 1(f), and so

$$1 + p_2 = S_2 = p_1 p_3^2 = 2(p_2 - 1)^2 = 8p_2^2 - 8p_2 + 2, \quad \text{or}$$

$$0 = 8p_2^2 - 9p_2 + 1 = (8p_2 - 1)(p_2 - 1),$$

which implies that p_2 is 1 or $1/8$; but neither of these numbers is prime.

This settles all possible cases, and proves Lemma 3. ■