



An Equation Involving the Totient: 10626

Florian Luca; Nasha Komanda

The American Mathematical Monthly, Vol. 106, No. 9. (Nov., 1999), pp. 869-870.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9890%28199911%29106%3A9%3C869%3AAEITT1%3E2.0.CO%3B2-S>

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/maa.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

For positive integers a, x, y with $a > 1$, it follows that $(a^x - 1)|(a^y - 1)$ if and only if $x|y$. When x and y are odd, we also have $(a^x + 1)|(a^y + 1)$ if and only if $x|y$.

Now let $S = \{2^{2^x-1} : x \in P\}$. For $x, y \in P$,

$$(2^{2^x-1} - 1)|(2^{2^y-1} - 1) \iff (2^x - 1)|(2^y - 1) \iff x|y.$$

Thus $(S, |)$ is isomorphic to $(P, |)$. Also

$$(2^{2^x-1})|(2^{2^y-1}) \iff (2^x - 1) \leq (2^y - 1) \iff x \leq y.$$

Thus $(S + 1, |)$ is isomorphic to (P, \leq) . Since $2^x - 1$ and $2^y - 1$ are odd, we have

$$(2^{2^x-1} + 1)|(2^{2^y-1} + 1) \iff (2^x - 1)|(2^y - 1) \iff x|y.$$

Thus $(S + 2, |)$ is isomorphic to $(P, |)$.

Solution to (b) by Robin J. Chapman, University of Exeter, Exeter, U. K. Such a T exists for all $n \in P$. Let $O = \{1, 3, 5, \dots\}$ be the set of odd positive integers. Let p_j denote the j -th smallest prime. Then $\phi : \prod_j p_j^{r_j} \rightarrow \prod_j p_{j+1}^{r_j}$ is an isomorphism from $(P, |)$ to $(O, |)$.

Given $n \in P$, let $T = nO = \{nm : m \in O\}$. Then $T + n = 2nP = \{2nk : k \in P\}$. The posets $(T, |)$ and $(O, |)$ are isomorphic, and $(T + n, |)$ and $(P, |)$ are isomorphic. We obtain $(T, |)$ isomorphic to $(T + n, |)$ by transitivity.

Part (a) solved also by R. J. Chapman (U. K.). Both parts solved also by J. Dawson (Australia), GCHQ Problems Group (U. K.), and the proposer.

An Equation Involving the Totient

10626 [1997, 871]. *Proposed by Florian Luca, Syracuse University, Syracuse, NY.* For a positive integer k , the number of positive integers less than k that are relatively prime to k is denoted $\phi(k)$.

(a) Show that if m and n are relatively prime positive integers, then $\phi(5^m - 1) \neq 5^n - 1$.

(b)* Find all positive integers m, n such that $\phi(5^m - 1) = 5^n - 1$.

Solution to (a) by Nasha Komanda, Central Michigan University, Mt. Pleasant, MI. We use the lemma proved in Problem **10623**: $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$ when a, m, n are positive integers.

When $\gcd(m, n) = 1$, the lemma yields $\gcd(5^m - 1, 5^n - 1) = 4$. When $5^m - 1$ has the prime factorization $2^{e_0} \prod_{i=1}^s p_i^{e_i}$ with all exponents positive, we have $\phi(5^m - 1) = 2^{e_0-1} \prod_{i=1}^s p_i^{e_i-1} (p_i - 1)$. Suppose that $\phi(5^m - 1) = 5^n - 1$. Since $\gcd(5^m - 1, 5^n - 1) = 4$, we have $e_i = 1$ for $1 \leq i \leq s$.

If m is even, then $5^m - 1 = 25^{m/2} - 1$ is divisible by 8. Therefore, $e_0 \geq 3$. Since m and n are relatively prime, n is odd, so $5^n - 1 \equiv 4 \pmod{8}$, which implies that $e_0 - 1 + s \leq 2$. Thus $e_0 = 3$ and $s = 0$, which yields the impossibility $5^m - 1 = 8$.

Thus m is odd, which yields $e_0 = 2$. Since $e_i = 1$ for $1 \leq i \leq s$, we have $5^m - 1 = 4 \prod_{i=1}^s p_i$. Thus $5^m \equiv 1 \pmod{p_i}$ for $1 \leq i \leq s$. Since m is odd, 5 is a quadratic residue modulo p_i . By the Quadratic Reciprocity Law, each p_i is a quadratic residue modulo 5. Thus $p_i \equiv \pm 1 \pmod{5}$. If $p_i \equiv 1 \pmod{5}$, then $p_i - 1 \equiv 0 \pmod{5}$ and $5^n - 1 \equiv 0 \pmod{5}$, which is impossible. Therefore, $p_i \equiv -1 \pmod{5}$ for $1 \leq i \leq s$. Our formula for $5^m - 1$ now yields $-1 \equiv (-1)^{s+1} \pmod{5}$, and hence s is even.

On the other hand, $e_i = 1$ for $1 \leq i \leq s$ also yields $5^n - 1 = 2 \prod_{i=1}^s (p_i - 1)$. With $p_i \equiv -1 \pmod{5}$, this yields $-1 \equiv 2(-2)^s \pmod{5}$. This requires $s \equiv 3 \pmod{4}$, which contradicts our conclusion that s is even. Thus m can be neither odd nor even, and no solution exists.

Editorial comment. No solution was received to part (b). Roy Barbara provided partial results about the general equation $\phi(a^m - 1) = a^n - 1$, with additional partial results in

the special case $a = 5$. When a is even, there is no solution except $(a, m, n) = (2, 1, 1)$. When a is odd and at least 3, there is no solution when n is odd, when m is a power of 2, or when m is divisible by at least as high a power of 2 as n .

When $a = 5$, further exclusions restrict the possibilities for (m, n) to $\{(2^k p, 2^k q) : p \text{ is odd, } q \text{ is even, and } 0 \leq k \leq 4\}$. Furthermore, such a solution requires the five equations $\phi(5^{2^j p} - 1) = 5^{2^j q} - 1$ for $0 \leq j \leq 4$. This is highly restrictive; there may be no solution.

Part (a) solved also by H. Salle, GCHQ Problems Group, and the proposer.

Three Congruent Circles Between Two Triangles

10659 [1998, 366]. *Proposed by Jiro Fukuta, Shinsei-cho, Gifu-ken, Japan.* Let D, E, F be points in the interior of sides BC, CA, AB , respectively, of triangle $\triangle ABC$ such that the incircles of $\triangle AEF, \triangle BFD$, and $\triangle CDE$ are congruent, each having radius r . Let ρ, s , and K be the inradius, semiperimeter, and area of $\triangle ABC$, and ρ', s' , and K' be the corresponding quantities for $\triangle DEF$.

(a) Prove that $\rho' = \rho - r, s' = (1 - r/\rho)s$, and $K' = (1 - r/\rho)^2 K$.

(b) Prove that, if $r = \rho/2$, then D, E , and F are midpoints of the sides of $\triangle ABC$.

Solution of part (a) by GCHQ Problems Group, Cheltenham, U. K. Let the incentres of $\triangle AEF, \triangle BFD$, and $\triangle CDE$ be O_1, O_2 , and O_3 respectively. We first show that the triangles $\triangle O_1 O_2 O_3$ and $\triangle DEF$ have the same area and same perimeter.

Let the incircle of $\triangle AEF$ touch AF at T and EF at U . Let the incircle of $\triangle BDF$ touch BF at V and DF at W . Then $FT = FU$ and $FV = FW$, so $FU + FW = FT + FV = TV = O_1 O_2$. Continuing this process around $\triangle DEF$ shows that it has the same perimeter as $\triangle O_1 O_2 O_3$.

Let G be the foot of the perpendicular from F to $O_1 O_2$ and let H be the intersection of $O_1 O_2$ and EF . Then $\text{Area}(\triangle FGO_1) = \text{Area}(\triangle FTO_1) = \text{Area}(\triangle FOU_1)$, so $\text{Area}(\triangle FGH) = \text{Area}(\triangle O_1 UH)$. Continuing in this manner shows that $\triangle DEF$ has the same area as $\triangle O_1 O_2 O_3$. The result is true whether or not line segments FG and $O_2 W$ intersect. Since the two triangles have the same area and the same perimeter, they must also have the same inradius, namely ρ' .

Now $\triangle O_1 O_2 O_3$ is homothetic to $\triangle ABC$, with the incentre of $\triangle ABC$ as the centre of homothety. It follows that $\rho' = \rho - r$. The scaling factor from $\triangle ABC$ to $\triangle O_1 O_2 O_3$ is ρ'/ρ , so $s' = (\rho'/\rho)s = (1 - r/\rho)s$ and $K' = (\rho'/\rho)^2 K = (1 - r/\rho)^2 K$ as required.

Solution of part (b) by Călin Popescu, Université Catholique de Louvain, Louvain-la-Neuve, Belgium. For brevity, let us call a triple of points D, E, F with the properties described in the statement of the problem r -adequate. The midpoints D_0, E_0, F_0 of the sides BC, CA, AB , respectively, form a $\rho/2$ -adequate triple; we have to show that it is the only such triple. To this end, let D, E , and F form a $\rho/2$ -adequate triple, and note that $K'/K = 1/4$, by part (a). Observe that $BD/BC, CE/CA$, and AF/AB can be written as $1/2 + x, 1/2 + y$, and $1/2 + z$, respectively, with x, y , and z either all in $(-1/2, 0]$ or all in $[0, 1/2)$. Indeed, if say $x < 0 < y$, then clearly the inradius of $\triangle CDE$ would be larger than the inradius of $\triangle CD_0 E_0$, which is impossible since both are $\rho/2$. Writing K_A, K_B, K_C for the areas of $\triangle AEF, \triangle BFD, \triangle CDE$, respectively, we obtain $K_A/K = (AE/AC)(AF/AB) = (1/2 - y)(1/2 + z) = 1/4 + (z - y)/2 - yz$ and similarly $K_B/K = 1/4 + (x - z)/2 - zx$ and $K_C/K = 1/4 + (y - x)/2 - xy$. It follows that $K'/K = 1 - (K_A/K + K_B/K + K_C/K) = 1/4 + xy + yz + zx$. Since x, y , and z are either all nonnegative or all nonpositive, $K'/K = 1/4$ forces $x = y = z = 0$. Hence D, E , and F are indeed the midpoints of the sides of the triangle ABC .

Solved also by T. Hermann, N. Lakshmanan, G. Peng, C. R. Pranesachar (India), A. Sasane (The Netherlands), and the proposer. Part (a) solved also by R. Barbara (France), F. Bellot Rosado (Spain), J. Dou (Spain), P. E. Nuesch (Switzerland), C. Popescu (Belgium), W. Reyes (Chile), R. A. Simon (Chile), and I. Sofair.