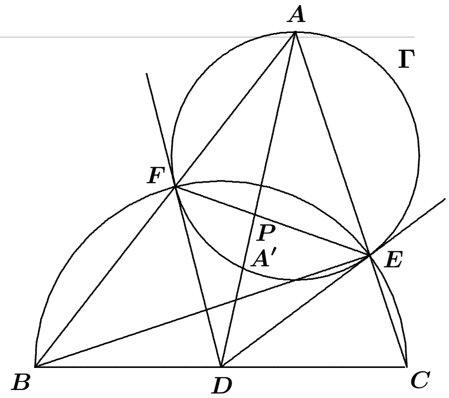
Let Γ be the circumcircle of $\triangle AEF$. By the Tangent-Chord Theorem, we see that DF is tangent to Γ at F and that DE is tangent to Γ at E. Let A' be the second point of intersection of DA with Γ. Applying the above lemma to Γ, we obtain

$$\frac{2}{DP} = \frac{1}{DA'} + \frac{1}{DA}. \qquad (3)$$



Let $r = DB = DE = DF$. Then $DA' \cdot DA = r^2$. Since we are given that $AD = \sqrt{3}r$, we deduce that $DA' = r/\sqrt{3}$. From (3), we have

$$\frac{2}{DP} = \frac{\sqrt{3}}{r} + \frac{1}{\sqrt{3}\,r}.$$

Therefore, $DP = (\sqrt{3}/2)r = \frac{1}{2}DA$, which means that P is the mid-point of AD.

[*Ed.:* By refining the argument at the end of the proof, one can show that $AD = \frac{\sqrt{3}}{2}BC$ if and only if P is the mid-point of AD.

The above proof assumes that $\triangle ABC$ is acute-angled. However, if there is an obtuse angle at B or at C, the result is still valid. The above proof extends to this case by simply modifying the argument used to show that DE and DF are tangent to Γ.]

3137. [2006 : 173, 176] *Proposed by Tina Balfour and Edward T.H. Wang, Wilfrid Laurier University, Waterloo, ON.*

Find all solutions in non-negative integers to the following Diophantine equations:

(a) $5^m + 3^m = 2^k$; (b) ★ $5^m + 3^n = 2^k$.

(a) *Composite of similar solutions by Brian D. Beasley, Presbyterian College, Clinton, SC, USA; and David E. Manes, SUNY at Oneonta, Oneonta, NY, USA.*

Note first that there are no solutions when $k = 0$. It is also clear that $(m, k) = (0, 1)$ and $(1, 3)$ are solutions. We now show that there are no other solutions.

Suppose $m \geq 2$. Then $k \geq 6$. Since $2^k \equiv 0 \pmod{16}$ for $k \geq 4$, we have $5^m + 3^m \equiv 0 \pmod{16}$.

However, the least non-negative residues of 5^m modulo 16 for $m \geq 1$ are 5, 9, 13, and 1, which repeat in cycles of length 4, while those of 3^m are 3, 9, 11, and 1, which also repeat in cycles of length 4. Consequently, $5^m + 3^m \equiv 8 \pmod{16}$ or $5^m + 3^m \equiv 2 \pmod{16}$, and our claim follows.

(b) *Solution by Mercedes Sánchez Benito, Universidad Complutense, Madrid, Spain, Óscar Ciaurri Ramírez, Universidad de La Rioja, Logroño, Spain, and Manuel Benito Muñoz and Emilio Fernández Moral, IES Sagasta, Logroño, Spain, modified by the editor.*

If n is even, we have $5^m + 3^n \equiv 1^m + (-1)^n \equiv 2 \pmod 4$. Since $2^k \equiv 2 \pmod 4$ if and only if $k = 1$, the unique solution for n even is $m = n = 0$ and $k = 1$.

Let n be odd. For $m = 0$, we have to find solutions to $1 + 3^n = 2^k$. However, Leo Hebreus (or Levi ben Gerson, 14^{th} century) proved that for all $n > 2$, the integer $3^n \pm 1$ has an odd divisor; hence, the unique solution of $1 + 3^n = 2^k$ for $m = 0$ and n odd is $n = 1$ and $k = 2$.

Now we assume that $m > 0$. By considering the equation modulo 3, we obtain $(-1)^m \equiv (-1)^k \pmod 3$, which implies that m and k have the same parity. On the other hand, by examining the equation modulo 5, we get

$$2^k \equiv (-2)^n \equiv -2^n \equiv \pm 2 \pmod 5 ,$$

since n is odd. This implies that k is odd (and then so is m).

Now suppose that $m \geq 3$ and $n \geq 3$ (which means that $k \geq 7$). Setting $A = 22276800 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17$, we checked by a computer program that there are no solutions of $5^m + 3^n = 2^k$ modulo A for odd exponents $m \geq 3$, $n \geq 3$, and $k > 7$ (the checking is a "finite" problem, since $5^{51} \equiv 5^3 \pmod A$, $3^{243} \equiv 3^3 \pmod A$, and $2^{127} \equiv 2^7 \pmod A$). Therefore, we must have either $m = 1$ or $n = 1$.

Let $n = 1$. We must look for solutions of $5^m + 3 = 2^k$ (this problem was proposed on the XXII Spanish Mathematical Olympiad). Using the modulus $B = 65792 = 2^8 \cdot 257$, we again used a computer to search for solutions modulo B (again the checking is a "finite" problem, since $5^{256} \equiv 1 \pmod B$ and $2^{25} \equiv 2^9 \pmod B$; furthermore, 9 is the smallest power of 2 where the remainders modulo B begin to repeat). The computer program yielded the following four cases for $n = 1$ and $m > 0$:

$$(m, k) \in \{(1, 3), (3, 7)\} .$$

Since the values for k lie in the non-periodic set of remainders of powers of 2 modulo B, we see that $k = 1$ or $k = 7$. This gives us the solutions $(m, n, k) = (1, 1, 3)$ and $(m, n, k) = (3, 1, 7)$. Furthermore, any other solutions must have $m \equiv 1 \pmod B$ or $m \equiv 3 \pmod B$. Since the smallest values for m other than 1 or 3 are significantly too large to have a solution, these are the only solutions for $n = 1$.

Lastly, we will examine $m = 1$ and $n \geq 3$. This time, we use the modulus $C = 2^6 \cdot 3^4 \cdot 17$ for our computer check. Once more this becomes a finite problem since $3^{21} \equiv 3^5 \pmod C$ and $2^{223} \equiv 2^7 \pmod C$; furthermore, 5 and 7 are the smallest powers of 3 and 2, respectively, where the remainders begin to repeat. The only solution modulo C that the program generated was $(n, k) = (3, 5)$. This yields the solution $(m, n, k) = (1, 3, 5)$. Since the powers on both 2 and 3 are in the non-periodic set of remainders of their respective powers, there are no further solutions.

In conclusion, there are exactly five solutions to $5^m + 3^n = 2^k$, namely:

$$(m,n,k) \ \in \ \{(0,0,1),\ (0,1,2),\ (1,1,3),\ (3,1,7),\ (1,3,5)\}\,.$$

Part (a) *also solved by MICHEL BATAILLE, Rouen, France; ROY BARBARA, Lebanese University, Fanar, Lebanon; MERCEDES SÁNCHEZ BENITO, Universidad Complutense, Madrid, Spain, ÓSCAR CIAURRI RAMÍREZ, Universidad de La Rioja, Logroño, Spain, and MANUEL BENITO MUNOZ ˜and EMILIO FERNÁNDEZ MORAL, IES Sagasta, Logroño, Spain; CHIP CURTIS, Missouri Southern State University, Joplin, MO, USA; RICHARD I. HESS, Rancho Palos Verdes, CA, USA; WALTHER JANOUS, Ursulinengymnasium, Innsbruck, Austria; JOEL SCHLOSBERG, Bayside, NY, USA; LI ZHOU, Polk Community College, Winter Haven, FL, USA; and the proposer.*

Beasley conjectured that the equation in part (b) *has exactly the five solutions which are determined above.*

The reason for the late featuring of this solution is that we wanted to have the computer solution properly analyzed. We apologize for this delay. We would appreciate if our readers could find a proof for the result which is independent of computer verification.

3139. [2006 : 238, 240; 2007 : 242] *Proposed by Michel Bataille, Rouen, France.*

Let ε be the ellipse $\frac{x^2}{a^2}+\frac{y^2}{b^2}-1=0$. Two parallel tangents to ε intersect a third tangent at $M_1(x_1,y_1)$ and $M_2(x_2,y_2)$. Show that the value of

$$\left(\frac{x_1^2}{a^2}+\frac{y_1^2}{b^2}-1\right)\left(\frac{x_2^2}{a^2}+\frac{y_2^2}{b^2}-1\right)$$

is independent of the chosen tangents.

II. *Solution by J.A. Thas, Ghent University, Ghent, Belgium.*

The desired result is a consequence of properties of projective coordinates interpreted in the affine plane. Our conic defines a *scalar product* between the points $M_1=(x_1,y_1)$ and $M_2=(x_2,y_2)$ by

$$\langle M_1,M_2\rangle \ = \ \frac{x_1x_2}{a^2}+\frac{y_1y_2}{b^2}-1\,.$$

There is likewise a scalar product defined by the dual conic (composed of the tangents to the conic) between pairs of lines: if $L_i=[u_i,v_i,w_i]$ represent the lines $u_ix+v_iy+w_i=0$ for $i=1$ and $i=2$, then

$$[L_1,L_2] \ = \ a^2u_1u_2+b^2v_1v_2-w_1w_2\,.$$

A pair of points or a pair of lines are conjugate if and only if their scalar product is zero. One easily shows that the line joining M_1 to M_2 is tangent to the conic if and only if

$$\langle M_1,M_1\rangle\langle M_2,M_2\rangle-\langle M_1,M_2\rangle^2 \ = \ 0\,. \qquad (1)$$