Solution to **Problem C** in the March 2015 issue of the NAW

José Hernández Santiago

Problem C. Determine all pairs (p, q) of odd primes with $q \equiv 3 \pmod 8$ such that $\frac{1}{p}(q^{p-1} - 1)$ is a perfect square.

CLAIM. The pair $(p = 5, q = 3)$ is the only one that satisfies the given constraints.

Proof. Let us suppose that

$$\frac{1}{p}(q^{p-1} - 1) = n^2$$

for some $n \in \mathbb{N}$. Then, if we write p as $2k + 1$ the above equation becomes

$$(q^k - 1)(q^k + 1) = p \cdot n^2. \tag{1}$$

Since $(q^k - 1, q^k + 1) = 2$, we have that $q^k - 1 = 2A$ and $q^k + 1 = 2B$ for some coprime natural numbers A and B: from this and the equation (1) we obtain that

$$4AB = p \cdot n^2$$

and whence

$$AB = p(n/2)^2.$$

This equation indicates that we must analyze the following two cases separately:

$$\textbf{Case I}.\ p|A \text{ and } p \nmid B \qquad \text{and} \qquad \textbf{Case II.}\ p \nmid A \text{ and } p|B.$$

Case I. If $A = p \cdot \ell_1$ then $(\ell_1, B) = 1$ and this implies, in the light of (2), that both ℓ_1 and B are perfect squares. Hence, we have in this case that

$$q^k - 1 = 2(p \cdot M^2) \qquad \text{and} \qquad q^k + 1 = 2N^2$$

for some $M, N \in \mathbb{N}$. The second equality in the previous line implies that 2 is a quadratic residue modulo q, which is plainly **absurd** because

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = -1.$$

Case II. If $B = p \cdot \ell_2$ then, proceeding as in the previous case, we obtain that both A and ℓ_2 are perfect squares. Hence,

$$q^k - 1 = 2\mathcal{M}_1^2 \qquad \text{and} \qquad q^k + 1 = 2(p \cdot N_1^2)$$

for some $\mathcal{M}_1, N_1 \in \mathbb{N}$.

There are two subcases to consider here:

Subcase 1: $3|\mathcal{M}_1$. It follows that $q^k \equiv 1 \pmod 3$ and that 3 can't be a divisor of q. Fermat's Little Theorem allows us to ascertain that $q^2 \equiv 1 \pmod 3$. Then, we have that $k = 1$ or $k = 2\ell$ for some $\ell \in \mathbb{N}$. The former possibility is ruled out easily by resorting to the equality $q^k + 1 = 2(p \cdot N_1^2) = 2(2k+1)N_1^2$. The latter possibility implies that

$$(q^\ell - 1)(q^\ell + 1) = 2\mathcal{M}_1^2. \tag{2}$$

The greatest common divisor of $q^\ell - 1$ and $q^\ell + 1$ is 2 and this allows us to write $q^\ell - 1 = 2a$ and $q^\ell + 1 = 2b$ for some coprime natural numbers a and b. Substituting this back into (2), we get

$$2ab = \mathcal{M}_1^2$$

which implies that $\mathcal{M}_1 = 2\mathcal{M}_2$ for some $\mathcal{M}_2 \in \mathbb{N}$ and whence

$$ab = 2\mathcal{M}_2^2.$$

Since a and b are relatively prime, the previous equation implies that either $2|a$ and $2 \nmid b$ or $2 \nmid a$ and $2|b$. In the first scenario we obtain that $q^\ell + 1 = 2T^2$ for some $T \in \mathbb{N}$, which is **absurd** (2 is not a quadratic residue modulo q). In the second one, we conclude that $q^\ell + 1 = 4T^2$ for some $T \in \mathbb{N}$. This implies in turn that $q^\ell = (2T-1)(2T+1)$: since q is an odd prime number, it can't divide $2T - 1$ and $2T + 1$ simultaneously. Hence $T = 1$ and $q = 3$, which is also **absurd**.

Subcase 2: $3 \nmid \mathcal{M}_1$. Then $q^k = 2\mathcal{M}_1^2 + 1 \equiv 0 \pmod 3$ and this implies that $q = 3$. The equation in (1) becomes

$$(3^k - 1)(3^k + 1) = p \cdot n^2. \tag{3}$$

The greatest common divisor of $3^k - 1$ and $3^k + 1$ is 2 and this allows us to write $3^k - 1 = 2c$ and $3^k + 1 = 2d$ for some coprime natural numbers c and d. Substituting this back into (3), we get that

$$cd = p(n/2)^2.$$

Once again, we have two subcases to consider:

Subcase 2.1: $p|c$ and $p \nmid d$. Proceeding as in **Case I** above, we conclude in this subcase that $3^k - 1 = 2(p \cdot \mathcal{M}_3^2)$ and $3^k + 1 = 2\mathcal{M}_4^2$ for some natural numbers $\mathcal{M}_3$ and $\mathcal{M}_4$. The latter equality **contradicts** the fact that 2 is a quadratic non-residue modulo 3.

Subcase 2.2: $p \nmid c$ and $p|d$. In this subcase we obtain that $3^k - 1 = 2\mathcal{M}_5^2$ and $3^k + 1 = 2(p \cdot \mathcal{M}_6^2)$ for some natural numbers $\mathcal{M}_5$ and $\mathcal{M}_6$. According to a celebrated result attributed to T. Nagell and W. Ljunggren[1], the equation

$$\frac{3^k - 1}{3 - 1} = \mathcal{M}_5^2$$

admits only one solution in the range $k > 2$: namely, $k = 5$ and $\mathcal{M}_5 = 11$. This leads to the conclusion that $p = 11$ and $q^{p-1} - 1 = 3^{10} - 1 = 59048$; nevertheless, the pair $(11, 3)$ is inadmissible because $59048/11 = 5368$ is not a perfect square.

It remains to determine if we get a *valid* pair (p, q) when $k = 1$ or $k = 2$. If $k = 1$ then $p = 3$; since we have that $q = 3$, p doesn't even divide $q^{p-1} - 1$ in this case. If $k = 2$ then $p = 5$ and whence

$$\frac{3^{5-1} - 1}{5} = \frac{(3^2 - 1)(3^2 + 1)}{5} = 8 \cdot 2 = 16 = 4^2.$$

The validity of our initial CLAIM follows now from the exhaustive analysis which we have just completed. □

[1] See, for instance, the introduction to this paper: Y. Bugeaud & P. Mihăilescu, *On the Nagell-Ljunggren equation* $\frac{x^n-1}{x-1} = y^q$. Math. Scand. 101 (2007), pp. 177–183. Bugeaud and Mihăilescu mention therein that, building on previous work of T. Nagell (and K. Mahler), W. Ljunggren proved in a 1943 paper published in the *Norsk Matematisk Tidsskrift* that the Diophantine equation

$$\frac{x^n - 1}{x - 1} = y^2$$

doesn't admit solutions in integers $x > 1, y > 1, n > 2$ except when $n = 4$, $x = 7$ and $n = 5$, $x = 3$. Additionally, it is noteworthy that the resolution of the Diophantine equation $3^m = 2n^2 + 1$ in nonnegative integers m and n was the subject matter of Problem 10873 of *The American Mathematical Monthly.* The solution chosen by the editors of the Problems and Solutions section of *the Monthly* depended on basic facts about Pell equations. The exact reference is: B. J. Venkatachala and Doyle Henderson, An exponential Diophantine equation: 10873, *Amer. Math. Monthly* Vol. 110, No. 3 (March 2003), p. 243.