# On Le's and Bugeaud's papers about the equation $ax^2 + b^{2m-1} = 4c^p$

Yuri Bilu

Denote by $h(-D)$ the class number of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{-D}\right)$. Le [3] claimed to prove that the equation

$$ax^2 + b^{2m-1} = 4c^p \tag{1}$$

has finitely many solutions $(a, b, c, x, m, p)$, where $a, b, c, x, m$ are positive integers and $p > 5$ is a prime number satisfying

$$\gcd(ax, b) = 1 \quad \text{and} \quad h(-ab) \not\equiv 0 \bmod p. \tag{2}$$

Le also gave an explicit upper bound for the solutions, subsequently reduced by Mignotte [4]. Recently, Bugeaud [2] gave the complete list of solutions.

Unfortunately, Le's claim (and *a fortiori* Bugeaud's result) are false in the form they are formulated. Here is a simple example. Put

$$\alpha = (1+\sqrt{-7})/2, \quad \beta = (1-\sqrt{-7})/2, \quad x_n = \alpha^n + \beta^n, \quad y_n = (\alpha^n - \beta^n)/\sqrt{-7}.$$

Then, for each odd prime $p$, the positive integers

$$a = 1, \quad b = 7y_p^2, \quad c = 2, \quad x = x_p, \quad m = 1$$

satisfy both (1) and (2).

Indeed, the only non-obvious point is $\gcd(ax, b) = 1$. It suffices to show that $\gcd(x_n, y_n) = 1$. In the ring $\mathcal{O}_K$ of integers of the field $K = \mathbb{Q}(\sqrt{-7})$ we have $\gcd(\alpha, \beta) = 1$ and both $\alpha$ and $\beta$ divide 2. It follows that $\gcd(x_n, 2) = 1$. On the other hand, $\gcd(x_n, y_n) \mid \gcd(2\alpha^n, 2\beta^n) = 2$, which implies that $\gcd(x_n, y_n) = 1$.

The problem is that the numbers $X_1, Y_1$ defined in the beginning of Section 3 of [3] need not be integers. At least, I see no way to show that they are integers without making additional assumptions. A natural assumption under which the results of Le and Bugeaud become valid is

$$b \text{ is square-free.} \tag{3}$$

Below I sketch an argument showing that (1) has only finitely many solutions satisfying (2) and (3).

The key role belongs to the following lemma. It is certainly known, but I have never seen a complete proof in the available literature.

**Lemma 1.** *Let $a, b, x, y$ be positive integers, with $a$ and $b$ square-free and*

$$\gcd(ax, by) = 1. \tag{4}$$

*Assume that*

$$ax^2 + by^2 = 4c^n, \tag{5}$$

*where $c$ and $n$ are positive integers such that* $\gcd(n, 6h(-ab)) = 1$. *Then there exist integers $x_1$ and $y_1$ such that*

$$\frac{x\sqrt{a} + y\sqrt{-b}}{2} = \left(\frac{x_1\sqrt{a} + y_1\sqrt{-b}}{2}\right)^n.$$

The proof of the lemma is based on the following obvious fact. Set $K = \mathbb{Q}(\sqrt{-ab})$ and $M = \left\{u\sqrt{a} + v\sqrt{-b} : u, v \in \mathbb{Q}\right\}$. Then

$$\text{for } \kappa \in K \text{ and } \mu \in M \text{ one has } \mu^2 \in K \text{ and } \kappa\mu \in M. \tag{6}$$

*Proof of Lemma 1.* The numbers

$$\alpha_n := \frac{x\sqrt{a} + y\sqrt{-b}}{2} \quad \text{and} \quad \bar{\alpha}_n := \frac{x\sqrt{a} - y\sqrt{-b}}{2}$$

are algebraic integers because they are roots of the polynomial $P(T) = T^4 + (2c^n - by^2)T^2 + c^{2n}$. Also, $\gcd(\alpha_n, \bar{\alpha}_n) = 1$ by (4). Hence $\alpha_n^2$ and $\bar{\alpha}_n^2$ are co-prime elements of the ring $\mathcal{O}_K$, where, as above, $K = \mathbb{Q}(\sqrt{-ab})$.

Since $\alpha_n^2\bar{\alpha}_n^2 = (c^2)^n$, we have $\left(\alpha_n^2\right) = \mathfrak{a}^n$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. Since $\gcd(n, h(-ab)) = 1$, we have $\alpha_n^2 = \eta\gamma^n$, where $\gamma \in \mathcal{O}_K$ and $\eta$ is a unit of $\mathcal{O}_K$. Since $\gcd(n, 6) = 1$, the unit $\eta$ is an $n$-th power of another unit. Hence $\alpha_n^2 = \gamma_1^n$ for some $\gamma_1 \in \mathcal{O}_K$.

Now put $\alpha = \alpha_n\gamma_1^{(1-n)/2}$. Then $\alpha \in M$ by (6), and $\alpha^{2n} = \alpha_n^2$, which implies $\alpha^n = \pm\alpha_n$. Replacing, if necessary, $\alpha$ by $-\alpha$, we obtain $\alpha^n = \alpha_n$ (recall that $n$ is odd).

Since $\alpha \in M$, we may write $\alpha = \left(x_1\sqrt{a} + y_1\sqrt{-b}\right)/2$ with $x_1, y_1 \in \mathbb{Q}$. It remains to show that $x_1, y_1 \in \mathbb{Z}$. Since $\alpha$ is an algebraic integer, $ax_1 = \mathrm{Tr}(\alpha\sqrt{a}) \in \mathbb{Z}$. Hence the denominator of the rational number $x_1$ divides $a$. Similarly, the denominator of $y_1$ divides $b$. Since $a$ and $b$ are co-prime and square-free, the denominator of $ax_1^2 + by_1^2$ is equal to the product of the denominators of $x_1$ and $y_1$. On the other hand, both the numbers $\alpha$ and $\bar{\alpha} = \left(x_1\sqrt{a} - y_1\sqrt{-b}\right)/2$ are algebraic integers, which implies that $ax_1^2 + by_1^2 = 4\alpha\bar{\alpha} \in \mathbb{Z}$. Thus, both the denominators of $x_1$ and $y_1$ are 1, which completes the proof of the lemma. $\square$

Now fix a solution $(a, b, c, x, m, p)$ of (1) satisfying (2) and (3). Without loss of generality we may assume that $a$ is square-free. Applying the lemma with $n = p$ and $y = b^{m-1}$, we find integers $x_1, y_1$ such that

$$\frac{x\sqrt{a} + b^{m-1/2}}{2} = \left(\frac{x_1\sqrt{a} + y_1\sqrt{-b}}{2}\right)^n.$$

One easily verifies that the numbers

$$\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{-b}}{2} \quad \text{and} \quad \bar{\alpha} = \frac{x_1\sqrt{a} - y_1\sqrt{-b}}{2}$$

form a *Lehmer pair*, as defined in [1]. The corresponding $p$-th Lehmer number $(\alpha^p - \bar{\alpha}^p)/(\alpha - \bar{\alpha})$ is equal to $b^{m-1}/y_1$. In particular, all its prime divisors divide $(\alpha^2 - \bar{\alpha}^2)^2 = -x_1y_1ab$. Hence the above-mentioned Lehmer number has no primitive divisors. Now famous results of Schinzel and Stewart about primitive divisors of Lehmer numbers imply that there are only finitely many possibilities for the triple $(\alpha, \bar{\alpha}, p)$. Therefore (1) has only finitely many solutions satisfying (2) and (3). Using the results of [1], one can give the complete list of solutions, as Bugeaud did in [2].

## References


[1] Yu. Bilu, G. Hanrot, P. Voutier (with an appendix by M. Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew. Math.*, to appear.

[2] Y. Bugeaud, On some exponential Diophantine equations, *Monatsh. Math.*, **132** (2001), 93–97.

[3] M. Le, On the Diophantine Equation $D_1x^2 + D_2^m = 4y^m$, *Monatsh. Math.* **120** (1995), 121–125.

[4] M. Mignotte, On the diophantine equation $D_1x^2 + D_2^m = 4y^m$, *Portugal. Math.* **54** (1997), 457–460.



A2X, Université Bordeaux 1, 351 cours de la Libération, 33405 Talence cedex, France; e-mail `yuri@math.u-bordeaux.fr` .