ACTA ARITHMETICA
112.1 (2004)

The diophantine equation $x^2 = p^a \pm p^b + 1$

by

FLORIAN LUCA (Morelia)

1. Introduction. Recently, Szalay (see [11]) found all the solutions of the diophantine equation $x^2 = 2^L \pm 2^M \pm 2^N$ in nonnegative integers x, M, N, L. In this paper, we look at the title equation

$$x^2 = p^a + \varepsilon p^b + 1, \qquad \varepsilon \in \{\pm 1\}, \tag{1}$$

in positive integers x, p, a, b, with $a > b$, and p a prime number. By Szalay's results, it suffices to consider the case $p > 2$. The problem of determining all the integer solutions (x, t, a, b) with x, a, and b positive of the more general diophantine equation $x^2 = t^a + t^b + 1$ was posed by Zachary Franco at the 1994 West Coast Number Theory Conference in Asilomar (see Problem 94:23 on the Problem Sets of this Conference), and various remarks on this equation (mostly pertaining to the case $t = 2$, which meanwhile has been completely solved by Szalay) are available from Gerry Myerson.

Before giving the main result, let us make a few remarks about the *degenerate cases* which we are not considering here, namely when either $a = b$, or $b = 0$. When $a = b$, equation (1) with $\varepsilon = -1$ has the positive integer solution $x = 1$ independently of p, while (1) with $\varepsilon = 1$ is of the form $x^2 - 1 = 2p^a$, which does not have integer solutions because $x^2 - 1$ cannot be an integer congruent to 2 modulo 4. When $b = 0$, equation (1) with $\varepsilon = -1$ becomes $x^2 = p^a$, which has the positive integer solution $x = p^{a/2}$ whenever a is even, while (1) with $\varepsilon = 1$ is of the form $x^2 - 2 = p^a$. It is known (see [10]) that this last diophantine equation has only finitely many positive integer solutions (x, p, a) with $a \geq 2$, and x can be bounded by an explicitly computable constant, which can be found using Baker's theory of lower bounds for linear forms in logarithms of algebraic numbers. It is not known whether this last equation has finitely or infinitely many solutions with $a = 1$, although the standard conjecture here is that there should be infinitely many prime numbers p of the form $x^2 - 2$.

2000 *Mathematics Subject Classification*: Primary 11D61, 11D72.

Our result is the following.

Theorem. *The only solutions of* (1) *in positive integers* (x, p, a, b), *with* $a > b$, *and* p *an odd prime number are* $(x, p, a, b) = (5, 3, 3, 1), (11, 5, 3, 1)$.

2. The equation $x^2 = y^{2a_1} \pm y^b \pm 1$.

In this section, we prove that the diophantine equation

$$x^2 = y^a + \varepsilon_1 y^b + \varepsilon_2, \qquad \varepsilon_1, \varepsilon_2 \in \{\pm 1\}, \tag{2}$$

has no positive integer solutions with $a > b$, a even, and $y > 2$ and not a perfect power of some other integer.

Case 1: *b is even.* With the substitution $X := x$, $Y := y^{b/2}$, $D := y^{a-b} + \varepsilon_1$ we may rewrite equation (2) as

$$X^2 - DY^2 = \varepsilon_2. \tag{3}$$

Since $a - b > 0$ is even, we see that $D = (y^{(a-b)/2})^2 + \varepsilon_1 > 1$ is not a perfect square, and therefore (3) is a Pell equation. The minimal positive integer solution (X_1, Y_1) of the Pell equation

$$X^2 - DY^2 = \pm 1$$

is certainly $(X_1, Y_1) = (y^{(a-b)/2}, 1)$ and

$$X_1^2 - DY_1^2 = -\varepsilon_1. \tag{4}$$

Since $Y = y^{b/2} > 1 = Y_1$, it follows that $(X, Y) = (X_t, Y_t)$ for some $t \geq 2$. Since $Y_2 = 2X_1Y_1 = 2y^{(a-b)/2}$ is a multiple of y, it follows from the well known properties of solutions of Pell equations that $2 \mid t$. In particular, $\varepsilon_2 = 1$, and $2 \mid Y_2 \mid Y_t$, and therefore y is even. If $t = 2$, we get $y^{b/2} = 2y^{(a-b)/2}$, therefore $y^{(2b-a)/2} = 2$, hence $y = 2$ and $b = (a + 2)/2$, but this is not a convenient solution for us because we are assuming that $y > 2$.

We now show that the case $t > 2$ does not lead to a solution either. Assume $t \geq 4$, and notice that any prime divisor p of $Y_t = y^{b/2}$ is already a prime divisor of $Y_2 = 2y^{(a-b)/2}$. Thus, the sequence $(Y_k)_k$, which is a *Lucas sequence of the first kind*, has the property that its tth term does not have a *primitive divisor*. From the results of Carmichael [3] (see also [2]), this is possible only when $t = 4, 6, 12$. Since both Y_4 and Y_6 divide Y_{12}, it suffices to treat the cases $t \in \{4, 6\}$. Letting $m := y^{(a-b)/2}$ and using the fact that

$$Y_t = \frac{(m + \sqrt{m^2 + \varepsilon_1})^t + (m - \sqrt{m^2 + \varepsilon_1})^t}{2\sqrt{m^2 + \varepsilon_1}}$$

for all positive integers t, one finds that $Y_2 = 2m$, $Y_4 = 4m(2m^2 + \varepsilon_1)$, and $Y_6 = 2m(16m^4 + 16\varepsilon_1 m^2 + 3)$. Since $m > 1$ and $2m^2 + \varepsilon_1 > 1$ is coprime to $2m$, it follows immediately that Y_4 is divisible by a prime p not dividing Y_2. Moreover, since $\gcd(2m, 16m^4 + 16\varepsilon_1 m^2 + 3) \mid 3$, the only instance in which all primes dividing Y_6 will also divide $2m$ is when $3 \mid m$ and $16m^4 + 16m^2\varepsilon_1 + 3$

is a power of 3. However, in this last case $16m^4 + 16\varepsilon_1 m^2 + 3 \equiv 3 \pmod 9$, and $16m^4 + 16\varepsilon_1 m^2 + 3 > 3$, so this is also impossible.

CASE 2: *b is odd.* In this case, with the substitution $X := x$, $Y := y^{(b-1)/2}$, $A := y$, $B := y^{a-b} + \varepsilon_1$, $D := AB = y(y^{a-b} + 1)$, we rewrite equation (2) as

$$X^2 - DY^2 = \varepsilon_2. \tag{5}$$

Since y is not a perfect square, and $A = y$ is coprime to $B = y^{a-b} + \varepsilon_1$, it follows that D is not a perfect square, therefore (5) is also a Pell equation.

If B is not a square, then the minimal positive integer solution (S, T) of the equation

$$AS^2 - BT^2 = \pm 1$$

is $(S_1, T_1) = (y^{(a-b-1)/2}, 1)$, for which $AS_1^2 - BT_1^2 = -\varepsilon_1$, and by the well known properties of solutions of Pell equations it follows that $\varepsilon_2 = 1$, and that the minimal positive integer solution of (5) is

$$X_1 + \sqrt{D}Y_1 = (S_1\sqrt{A} + T_1\sqrt{B})^2 = 2y^{a-b} + \varepsilon_1 + 2y^{(a-b-1)/2}\sqrt{D},$$

therefore $(X_1, Y_1) = (2y^{a-b} + \varepsilon_1, 2y^{(a-b-1)/2})$. Let $Y = Y_t$ for some $t \geq 1$. Since $Y_1 \mid Y_t$, it follows that $2y^{(a-b-1)/2} \mid y^{(b-1)/2}$, therefore $b > 1$ and y is even. If $t = 1$, it then follows that $y^{(b-1)/2} = 2y^{(a-b-1)/2}$, leading again to the conclusion that $y = 2$ and $b = (a+2)/2$, which is a case we are not considering. If $t > 1$, then every prime divisor of Y_t divides Y_1, and thus we are led again to the instance in which Y_t does not have a primitive divisor. By Carmichael's results, it follows that $t \in \{2, 3, 4, 5, 6, 12\}$. Since Y_2 divides all Y_4, Y_6 and Y_{12}, it suffices to show that Y_t has a prime divisor p not dividing y when $t \in \{2, 3, 5\}$. A similar computation as in the previous case shows that $Y_2 = 4y^{(a-b-1)/2}(2y^{a-b} + \varepsilon_1)$, $Y_3 = 2y^{(a-b-1)/2}(16y^{2(a-b)} + 16\varepsilon_1 y^{(a-b)/2} + 3)$, and by arguments similar to the previous ones one shows that not all prime divisors dividing either Y_2 or Y_3 can divide Y_1. Finally, when $t = 5$, a result of Carmichael from [3] (see also Table 1 of [2]) says that the only Lucas sequences with real roots which lack primitive divisors in their 5th term are *associated* with the Fibonacci sequence, i.e., their roots are of the form $\pm((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, while our Lucas sequence $(Y_k)_k$ has roots $2y^{a-b} + \varepsilon_1 \pm 2y^{(a-b-1)/2}\sqrt{y(y^{a-b} + \varepsilon_1)}$ which are not of the above type.

This was the case when B was not a perfect square. If $B = y^{a-b} + \varepsilon_1 = z^2$ is a perfect square, then $a - b = 1$. Indeed, if $a - b > 1$, then the above equation is a particular instance of Catalan's equation which has been treated a long time ago by V. A. Lebesgue [8] (for the case $\varepsilon_1 = -1$), and by Chao Ko [6] (for the case $\varepsilon_1 = 1$), and it has no positive integer solutions with $y > 2$. Finally, for the last case in which $a - b = 1$ and $y + \varepsilon_1 = z^2$ with some integer $z > 1$, we write $U := x$, $V := y^{(b-1)/2}z = (z^2 - \varepsilon_1)^{(b-1)/2}z$, and $D' := y = z^2 - \varepsilon_1$, and notice that equation (2) becomes

$$U^2 - D'V^2 = \varepsilon_2, \tag{6}$$

with $D' = y > 2$ not a square. The minimal positive integer solution of the Pell equation

$$U^2 - D'V^2 = \pm 1$$

is obviously $(U_1, V_1) = (z, 1)$ for which $U^2 - D'V^2 = \varepsilon_1$, and since $(U_2, V_2) = (2z^2 - \varepsilon_1, 2z)$ and $z \mid V$, it follows that $V = V_t$ for some even integer t. The case $t = 2$ gives $y^{(b-1)/2}z = 2z$, therefore $y = 2$ and $b = 3$, which is again not convenient, therefore we must have $t \geq 4$. Notice that

$$V_t = \frac{\alpha^t - \beta^t}{\alpha - \beta}, \quad \text{where} \quad (\alpha, \beta) := (z + \sqrt{z^2 - \varepsilon}, z - \sqrt{z^2 - \varepsilon}),$$

and the fact that $V_t = zy^{(b-1)/2} = zD'^{(b-1)/2}$ implies that every prime divisor of V_t divides either $V_2 = 2z$ or $D' = (\alpha - \beta)^2$. Thus, V_t is a *defective* Lucas number (in the terminology of [2]), and by Carmichael's results it follows again that the only possibilities for t are $t \in \{4, 6, 12\}$, and since $Y_4 \mid Y_{12}$ it suffices to show that this cannot happen for $t \in \{4, 6\}$. Now $Y_4 = 2z(2z^2 - \varepsilon)$ and $Y_6 = 2z(16z^4 - 16z^2\varepsilon + 3)$, and since $z > 1$ and $\gcd(2z(z^2 - \varepsilon), 2z^2 - \varepsilon) = 1$, and $\gcd(2z(z^2 - \varepsilon), 16z^4 - 16z^2\varepsilon + 3) = 3$, one checks again that it is not possible that all the prime factors of either Y_4 or Y_6 are also prime factors of $z(z^2 - \varepsilon)$, which concludes the proof.

From the above result, it follows that we may assume that a is odd in equation (1). We also notice that $a \geq 2b + 1$ must hold. Indeed, if not, then $a \leq 2b - 1$, and in particular $b \geq 2$. Rewriting (1) as $(x - 1)(x + 1) = p^b(p^{a-b} + \varepsilon)$, it follows that there exists $\varepsilon_1 \in \{\pm 1\}$ so that $x \equiv \varepsilon_1 \pmod{p^b}$. Since $x > 1$, it follows that $x \geq p^b - 1$, therefore

$$p^{2b-1} + p^b + 1 \geq p^a + \varepsilon p^b + 1 = x^2 \geq (p^b - 1)^2 = p^{2b} - 2p^b + 1,$$

which is equivalent to $3 > p^{b-1}(p - 1)$, which is impossible because $b \geq 2$ and $p \geq 3$.

3. The equation $x^2 = p^a + p^b + 1$ with a odd.

Looking at equation (1) with $\varepsilon = 1$ modulo 4, we see that the only case in which solutions might exist is when $p \equiv 3 \pmod 4$ and b is even. Write $p^b + 1 = Du^2$, with D squarefree and $u \geq 1$ some integer. Since b is even and p is odd, we see that $2 \,\|\, D$. We write $\mathbb{K} := \mathbb{Q}[\sqrt{D}]$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{D}]$ for the ring of algebraic integers in $\mathbb{K}$, and $\mathcal{O}' = \mathbb{Z}[\sqrt{D}\,u] = \mathbb{Z}[\sqrt{p^b + 1}]$. Rewriting the equation $p^b + 1 = Du^2$ as

$$(p^{b/2})^2 - Du^2 = -1 \tag{7}$$

we recognize that $(X, Y) = (p^{b/2}, u)$ is a solution of the Pell equation

$$X^2 - DY^2 = -1. \tag{8}$$

Lemma. *Let b be even, p be an odd prime, and write $p^b + 1 = Du^2$ with D squarefree. Then $(X, Y) = (p^{b/2}, u)$ is the minimal solution of the Pell equation*

$$X^2 - DY^2 = \pm 1 \tag{9}$$

except for $b = D = 2$ in which case $(X, Y) = (P, Q) = (p, u)$ is a solution of the Pell equation

$$P^2 - 2Q^2 = \pm 1. \tag{10}$$

In this case, if $t \geq 1$ is an integer and if we write (P_t, Q_t) for the tth solution of equation (10), then $(p, u) = (P_k, Q_k)$ with some odd prime number k.

Proof. Let $t \geq 1$ and (X_t, Y_t) be the tth solution of the Pell equation

$$X^2 - DY^2 = -1. \tag{11}$$

Since $(X, Y) = (X_t, Y_t)$ is a solution of (11) with the sign -1 on the right hand side, it follows that t is odd. By the results of Carmichael, X_t has primitive divisors for all odd values of t except $t \in \{3, 5\}$. By arguments entirely similar to the ones employed previously, one shows that X_t has primitive divisors (i.e., that there exists a prime number $p \mid X_t$ so that $p \nmid X_1$) when $t \in \{3, 5\}$ as well. Assume now that $X_t = p^{b/2}$ with some odd prime p, even positive integer b, and odd integer $t > 1$. Since $X_1 \mid X_t$, it follows that $X_1 = p^c$ with some nonnegative integer c. If $c \geq 1$, then X_t will not have a primitive divisor, which is impossible. Thus, $c = 0$, and therefore $(X_1, Y_1) = (1, Y_1)$ is a solution of the Pell equation $1^2 - DY_1^2 = -1$. This shows that $D = 2$ and that $(X_t, Y_t) = (P_k, Q_k)$ with some odd integer k. The fact that $b = 2$ must hold is Theorem 6.1 of [5] (see also Theorem 1.1 of [1] for a more general result), therefore $P_k = p$ is a prime, and since $P_d \mid P_k$ for all divisors d of k, we conclude that k is an odd prime.

Returning now to our original problem, we proceed by analysing each one of the two cases from the above lemma.

Case 1: $(X, Y) = (p^{b/2}, u)$ *is the minimal positive integer solution of the Pell equation* (8). In this case, the fundamental unit in $\mathcal{O}_{\mathbb{K}}$ is $\zeta := p^{b/2} + \sqrt{D}\,u = p^{b/2} + \sqrt{p^b + 1}$, which lives in the order $\mathcal{O}'$. We rewrite equation $p^b + 1 = Du^2$ as

$$p^b = Du^2 - 1 = -(1 + \sqrt{p^b + 1})(1 - \sqrt{p^b + 1}). \tag{12}$$

For any integer a and any odd prime q we write $(a|q)$ for the Legendre symbol of a with respect to q. Since $(D|p) = (Du^2|p) = (p^b + 1|p) = (1|p) = 1$, it follows that the principal ideal $[p]$ generated by p inside $\mathcal{O}_{\mathbb{K}}$ splits into a product of two prime ideals in $\mathcal{O}_{\mathbb{K}}$; we call them π_1 and π_2. Passing to ideals in (12), we get

$$\pi_1^b\pi_2^b = [1 - \sqrt{p^b + 1}][1 + \sqrt{p^b + 1}]. \tag{13}$$

The ideals appearing on the right hand side of (13) are obviously coprime (because if I is any ideal dividing both of them, then on the one hand I divides their product which is a power of p, and on the other hand I divides the sum $(1 + \sqrt{p^b + 1}) + (1 - \sqrt{p^b + 1}) = 2)$, therefore, by unique factorization, and up to relabelling π_1 and π_2, we may assume that

$$\pi_1^b = [1 + \sqrt{p^b + 1}], \qquad \pi_2^b = [1 - \sqrt{p^b + 1}]. \tag{14}$$

From (14), we see that π_1^b is principal and has a generator in $\mathcal{O}'$, and since the fundamental unit in $\mathcal{O}_{\mathbb{K}}$ is in $\mathcal{O}'$ as well, it follows that every generator of π_1^b is in $\mathcal{O}'$, and the same is true for π_2. Moreover, the order of π_1 in the ideal class group of $\mathbb{K}$ is a divisor of b. We now rewrite equation (1) with $\varepsilon = 1$ as

$$p^a = x^2 - (p^b + 1) = (x - \sqrt{p^b + 1})(x + \sqrt{p^b + 1}),$$

and pass again to ideals in $\mathcal{O}_{\mathbb{K}}$ to conclude that

$$\pi_1^a\pi_2^a = [x + \sqrt{p^a + 1}][x - \sqrt{p^a + 1}]. \tag{15}$$

The integer x is clearly coprime to p, and by an argument similar to the one employed previously, we conclude that the two principal ideals appearing on the right hand side of (15) are coprime. Thus, by unique factorization for ideals in $\mathcal{O}_{\mathbb{K}}$, there exists $\varepsilon_1 \in \{\pm 1\}$ so that

$$\pi_1^a = [x + \varepsilon_1\sqrt{p^b + 1}], \qquad \pi_2^a = [x - \varepsilon_1\sqrt{p^b + 1}]. \tag{16}$$

In particular, the order of π_1 in the ideal class group of $\mathbb{K}$ is a divisor of a, and since both the fundamental unit in $\mathcal{O}_{\mathbb{K}}$ as well as the generator $x + \varepsilon_1\sqrt{p^b + 1}$ of π_1^a are in $\mathcal{O}'$, all generators of π_1^a are in $\mathcal{O}'$. It now follows that if we write $c := \gcd(a, b)$, then π_1^c is principal, and every generator of π_1^c in $\mathcal{O}_{\mathbb{K}}$ belongs to $\mathcal{O}'$ as well. Since a is odd and b is even, we have $c \le b/2$. By writing $v + w\sqrt{p^b + 1}$ for some generator of π_1^c (here, v and w are nonzero integers with v and $w(p^b + 1)$ coprime), and computing norms, we get the diophantine equation

$$v^2 - w^2(p^b + 1) = \pm p^c. \tag{17}$$

With $m := p^{b/2}$, $D' := m^2 + 1$, and $z := p^c \le p^{b/2} < \sqrt{D'}$, we have obtained the diophantine equation

$$v^2 - w^2 D' = \pm z \quad \text{with } 1 < z < \sqrt{D'}, \tag{18}$$

and we may assume that v and w are both positive. It is well known that in this case v/w must be a convergent of $\sqrt{D'}$. Since $D' = m^2 + 1$, we find that the continued fraction of $\sqrt{D'}$ is $[m, \{2m\}]$, and if p_k/q_k is any convergent to $\sqrt{D'}$, then $p_k^2 - D'q_k^2 = \pm 1$. Thus, equation (18) does not have an integer solution (v, w, z) with v and wD' coprime and $1 < z < \sqrt{D'}$, which completes the analysis for this case.

Case 2: *$b = D = 2$, and $(p, u) = (P_k, Q_k)$ for some odd prime number k.* Notice that $a \geq 2b + 1 = 5$. When $k = 3$, we get $p = P_3 = 7$, and equation (1) becomes $x^2 = 7^a + 7^2 + 1$, which reduced modulo 5 gives $x^2 = 7^a \pmod 5$, which is impossible because $(7^a|5) = (7|5) = -1$. When $k = 5$, we get $p = P_k = 41$, which is congruent to 1 modulo 4, which is impossible. When $k = 7$, we get $P_k = 239$, and equation (1) becomes $x^2 = 239^a + 239^2 + 1$, which reduced modulo 13 gives $x^2 = 239^a \pmod{13}$, which is impossible because $(239|13) = (5|13) = (13|5) = (3|5) = -1$. When $k = 11$, then $P_k = 8119$ is a multiple of 23, therefore it is not prime. Thus, $k \geq 13$, therefore $p = P_k > 47000$. We now write $\mathbb{K} := \mathbb{Q}[\sqrt{2}]$, and $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ for the ring of algebraic integers in $\mathbb{K}$. The ring $\mathcal{O}_{\mathbb{K}}$ is Euclidean and its fundamental unit is $\zeta = 1 + \sqrt{2}$. From the equation

$$p^2 = P_k^2 = -1 + 2Q_k^2,$$

it follows that

$$p^2 = -(1 + Q_k\sqrt{2})(1 - Q_k\sqrt{2}).$$

We write $p = \pi_1 \cdot \pi_2$, where π_1 and π_2 are prime numbers in $\mathbb{Q}[\sqrt{2}]$, we rewrite (1) with $\varepsilon = 1$ as

$$p^a = x^2 - 2Q_k^2 = (x - Q_k\sqrt{2})(x + Q_k\sqrt{2}), \tag{19}$$

and we square both sides of (19) to get

$$\begin{aligned} -(1 + Q_k\sqrt{2})^a(1 - Q_k\sqrt{2})^a &= p^{2a} = \pi_1^{2a}\pi_2^{2a} \\ &= (x - Q_k\sqrt{2})^2(x + Q_k\sqrt{2})^2. \end{aligned} \tag{20}$$

By the unique factorization property in $\mathcal{O}_{\mathbb{K}}$, there exist integers l, ε_1, ε_2 with $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ so that

$$(1 + Q_k\sqrt{2})^a = \varepsilon_1(x + \varepsilon_2 Q_k\sqrt{2})^2\zeta^l. \tag{21}$$

The number l will turn out to be positive, but for the time being we do not work under this assumption. Conjugating (21) we get

$$(1 - Q_k\sqrt{2})^a = \varepsilon_1(x - \varepsilon_2 Q_k\sqrt{2})^2(-\zeta^{-1})^l. \tag{22}$$

Multiplying (21) and (22) and comparing the resulting equation with (20) shows that l must be an odd number. In particular, $|l| \geq 1$. We next give an upper bound on $|l|$ in terms of a. To start, we notice that

$$p - 1 < Q_k\sqrt{2} - 1 < Q_k\sqrt{2} + 1 < p + 2. \tag{23}$$

Indeed, if $Q_k\sqrt{2}-1<p-1$, then $Q_k\sqrt{2}+1<p+1$, therefore

$$p^2=(Q_k\sqrt{2}-1)(Q_k\sqrt{2}+1)<p^2-1,$$

which is impossible. The inequality $Q_k\sqrt{2}+1<p+2$ can be proved in a similar way. Let us also notice that

$$p^{(a-2)/2}(p-1)<x-Q_k\sqrt{2}. \tag{24}$$

Indeed, if (24) did not hold, then we would get

$$x\le p^{(a-2)/2}(p-1)+Q_k\sqrt{2}=p^{(a-2)/2}(p-1)+\sqrt{p^2+1},$$

therefore

$$\begin{aligned}p^a+p^2+1=x^2&\le (p^{(a-2)/2}(p-1)+\sqrt{p^2+1})^2\\&=p^a-2p^{a-1}+p^{a-2}+(p^2+1)+2p^{(a-2)/2}(p-1)\sqrt{p^2+1},\end{aligned}$$

which implies

$$2p^{a-1}-p^{a-2}<2p^{(a-2)/2}(p-1)\sqrt{p^2+1}<2p^{(a+2)/2},$$

therefore

$$p^{a-1}<2p^{a-1}-p^{a-2}<2p^{(a+2)/2},$$

hence,

$$p^{a-4}<4,$$

which is impossible for $p>47000$ and $a\ge 5$. From (23)–(24) and (21)–(22), we get

$$\begin{aligned}\zeta^{-|l|}\ge\frac{(x-Q_k\sqrt{2})^2}{(1+Q_k\sqrt{2})^a}&>\frac{p^{a-2}(p-1)^2}{(p+2)^a}=\left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}\right)^{-a}\\&>\left(1+\frac{2}{p}\right)^{-(a+2)}>\exp\left(-\frac{2(a+2)}{p}\right),\end{aligned}$$

therefore

$$|l|<\frac{2(a+2)}{p\log\zeta}. \tag{25}$$

A better inequality than (25) can be achieved by noticing that $k\,|\,l$. Indeed, write $l=\varepsilon_3|l|$ and (21) as

$$(1+Q_k\sqrt{2})^a=\varepsilon_1(x+\varepsilon_2Q_k\sqrt{2})^2(P_{|l|}+\varepsilon_3Q_{|l|}\sqrt{2}). \tag{26}$$

The coefficient of $\sqrt{2}$ on the left hand side of (26) is certainly a multiple of Q_k, while the coefficient of $\sqrt{2}$ on the right hand side of (26) is

$$\varepsilon_1(2\varepsilon_2xQ_kP_{|l|}+2\varepsilon_3Q_{|l|}Q_k^2+\varepsilon_3Q_{|l|}x^2), \tag{27}$$

and imposing that the number shown at (27) is a multiple of Q_k, we get $Q_k\,|\,Q_{|l|}x^2$. Since x and Q_k are obviously coprime, it follows that $Q_k\,|\,Q_{|l|}$, which shows that $k \mid l$. Thus, writing $|l| = sk$, we find that $s \geq 1$ is odd, and that

$$s < \frac{2(a+2)}{kP_k \log(1+\sqrt{2})}. \tag{28}$$

We now divide the two relations (21) and (22) side by side keeping in mind that l is odd to get

$$\left(\frac{1+Q_k\sqrt{2}}{1-Q_k\sqrt{2}}\right)^a \zeta^{-2l} = -\left(\frac{x+\varepsilon_2 Q_k\sqrt{2}}{x-\varepsilon_2 Q_k\sqrt{2}}\right)^2,$$

therefore with

$$\alpha := -\frac{1+Q_k\sqrt{2}}{1-Q_k\sqrt{2}},$$

we have

$$|\alpha^a \zeta^{-2l} - 1| = \left|\left(\frac{x+\varepsilon_2 Q_k\sqrt{2}}{x-\varepsilon_2 Q_k\sqrt{2}}\right)^2 - 1\right|. \tag{29}$$

Now

$$\left|\frac{x+\varepsilon_2 Q_k\sqrt{2}}{x-\varepsilon_2 Q_k\sqrt{2}} - 1\right| \leq \frac{2Q_k\sqrt{2}}{x-Q_k\sqrt{2}} < \frac{2\sqrt{p^2+1}}{p^{(a-2)/2}(p-1)} < \frac{3}{p^{(a-2)/2}},$$

therefore

$$\left|\left(\frac{x+\varepsilon_2 Q_k\sqrt{2}}{x-\varepsilon_2 Q_k\sqrt{2}}\right)^2 - 1\right| < \frac{6}{p^{(a-2)/2}} + \frac{9}{p^{a-2}} < \frac{7}{p^{(a-2)/2}}. \tag{30}$$

Thus, with (30), inequality (29) implies that

$$|\alpha^a \zeta^{-2l} - 1| < \frac{7}{p^{(a-2)/2}}. \tag{31}$$

We notice that both α and ζ are real, positive (in fact, larger than 1), and multiplicatively independent, and with $\Lambda := a\log\alpha - 2l\log\zeta$ inequality (31) becomes

$$|e^{\Lambda} - 1| < \frac{7}{p^{(a-2)/2}} < \frac{7}{p} < \frac{7}{40000}. \tag{32}$$

For real values of Λ for which (32) holds, the inequality $|e^{\Lambda} - 1| > |\Lambda|/2$ also holds, therefore (31) implies

$$|\Lambda| < \frac{14}{p^{(a-2)/2}},$$

which is equivalent to

$$\log|\Lambda| < \log 14 - \frac{a-2}{2}\log p. \tag{33}$$

We now need a lower bound for $\log|\Lambda|$, and we use the following one due to Laurent, Mignotte and Nesterenko (see Corollaire 2 in [7]).

Theorem LMN. *Let α_1, α_2 be real and positive algebraic numbers which are multiplicatively independent. Put $\mathbb{K} := \mathbb{Q}[\alpha_1, \alpha_2]$, $D := [\mathbb{K} : \mathbb{Q}]$, and assume that A_1 and A_2 are positive numbers such that*

$$\log A_i \geq \max\left\{ h(\alpha_i), \frac{|\log(\alpha_i)|}{D}, \frac{1}{D} \right\} \tag{34}$$

with $i := 1, 2$, where $h(\alpha)$ is the logarithmic height of the algebraic number α. For any two positive integers b_1 and b_2 put

$$b' := \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}, \tag{35}$$

and let

$$\Lambda := b_2 \log \alpha_2 - b_1 \log \alpha_1.$$

Then

$$\log |\Lambda| \geq -24.34 D^4 \left(\max\left\{ \log b' + 0.14, \frac{21}{D}, \frac{1}{2} \right\} \right)^2 \log A_1 \log A_2. \tag{36}$$

In our case $\alpha > 1$, $\zeta > 1$, and a is positive, therefore the only instance in which $|\Lambda|$ will be small is when l is also positive. We may put $\alpha_2 := \alpha$, $\alpha_1 := \zeta$, $b_2 := a$, and $b_1 := 2l$. In this case, $\mathbb{K} = \mathbb{Q}[\alpha_1, \alpha_2]$ is precisely $\mathbb{Q}[\sqrt{2}]$, therefore we may put $D := 2$. The conjugate of α_1 is $1 - \sqrt{2}$, therefore

$$h(\alpha_1) = h(1 + \sqrt{2}) = \frac{1}{2} \log(1 + \sqrt{2}),$$

while the conjugate of α_2 is α_2^{-1}, therefore its logarithmic height is

$$h(\alpha_2) = \frac{1}{2}\left(\log(2Q_k^2 - 1) + \log\left(\frac{\sqrt{2}\, Q_k + 1}{\sqrt{2}\, Q_k - 1} \right) \right) < \frac{\log(P_k^2) + \log 2}{2} < \log(2P_k).$$

Thus, we may choose A_1 and A_2 to be such that $\log A_1 = 1/2$, and $\log A_2 = \log(2p)$, and then inequalities (34) hold. Now

$$b' = \frac{2l}{2 \log A_2} + \frac{a}{2 \log A_1} < a + l < 2a,$$

with the last inequalities holding by (25) and the fact that p is large. Thus,

$$\begin{aligned} \log |\Lambda| &> -2^3 \cdot 24.34 \cdot (\max\{\log(2a) + 0.14, 10.5\})^2 \cdot \log(2p) \\ &> -200 \cdot (\max\{\log(2a) + 0.14, 10.5\})^2 \log(2p). \end{aligned} \tag{37}$$

Comparing (33) and (37) we get

$$-200 \cdot (\max\{\log(2a) + 0.14, 10.5\})^2 \log(2p) < \log 14 - \frac{a-2}{2} \log p,$$

therefore

$$a - 2 < \frac{2 \log 14}{\log p} + 400 \cdot (\max\{\log(2a) + 0.14, 10.5\})^2 \cdot \frac{\log(2p)}{\log p}. \tag{38}$$

Since $p > 47000 > 14^2$, we have $\log(2p)/\log p < 1.07$, and therefore (38) implies

$$a - 3 < 428(\max\{\log(2a) + 0.14, 10.5\})^2. \tag{39}$$

When $10.5 > 0.14 + \log(2a)$, (39) gives

$$a < 3 + 428 \cdot 10.5^2 < 50000,$$

while when $\log(2a) + 0.14 \geq 10.5$, it becomes

$$a - 3 < 428 \cdot (\log(2a) + 0.14)^2,$$

which implies that $a < 52000$. Thus, $a < 52000$, and now (28) tells us that

$$1 \leq s < \frac{2(52000 + 2)}{13 \cdot 47000 \cdot \log(1 + \sqrt{2})} < 1,$$

which is the final contradiction here.

4. The equation $x^2 = p^a - p^b + 1$. We first analyse the case of $b = 3a$. In this case, with $q := p^b$, the equation becomes $x^2 = q^3 - q + 1$. While this last equation is a particular instance of the equation $Y^2 = X^3 - X + 1$ which is an elliptic curve, and therefore all its integer solutions (X, Y) can be computed using various computer packages like SIMATH, for example, we show by an elementary argument that the only positive integer solutions (x, q) of our equation are $(x, q) = (5, 3), (11, 5)$.

Writing the equation as $(x - 1)(x + 1) = q(q^2 - 1)$, it follows that there exists $\varepsilon \in \{\pm 1\}$ so that $q \mid x - \varepsilon$. We write $x = q\lambda + \varepsilon$, with some positive integer λ, and the equation becomes $\lambda(q\lambda + 2\varepsilon) = q^2 - 1$, therefore $q\lambda^2 + (2\lambda\varepsilon + 1) = q^2$. We now learn that $q \mid 2\lambda\varepsilon + 1$, therefore there exists an odd positive integer w so that $2\lambda\varepsilon + 1 = \varepsilon q w$. Thus, $\lambda = (qw - \varepsilon)/2$, and we may rewrite our equation in terms of w to get

$$(qw - \varepsilon)^2 + 4\varepsilon w = 4q,$$

therefore

$$(qw - 1)^2 \leq 4(q - \varepsilon w) \leq 4(q + w) \leq 4(qw + 1),$$

and so,

$$(qw)^2 - 6qw - 3 < 0,$$

which implies $qw < 3 + 2\sqrt{3} < 7$. Thus, $q \in \{3, 5\}$, which leads to the positive integer solutions $(x, q) = (5, 3), (11, 5)$.

From now on, we assume that a is odd, $a > 2b + 1$, $a \neq 3b$. We write $p^b - 1 = Du^2$, with D and u positive integers, and D squarefree. We write $\mathbb{K} := \mathbb{Q}[i\sqrt{D}]$, $\mathcal{O}_{\mathbb{K}}$ for the ring of algebraic integers in $\mathbb{K}$, and we notice that $p^b = (1 + i\sqrt{D}\,u)(1 - i\sqrt{D}\,u)$. By the usual argument, the two principal ideals $[1 + i\sqrt{D}\,u]$ and $[1 - i\sqrt{D}\,u]$ are coprime in $\mathcal{O}_{\mathbb{K}}$, and the principal ideal $[p]$ generated by p inside $\mathcal{O}_{\mathbb{K}}$ splits into two prime ideals; we call them

π_1 and π_2. By unique factorization for ideals in $\mathcal{O}_{\mathbb{K}}$, we may assume that $\pi_1^b = [1 + i\sqrt{D}\,u]$ and $\pi_2^b = [1 - i\sqrt{D}]$. In particular, the order of π_1 in the ideal class group of $\mathbb{K}$ is a divisor of b, and the same is true for π_2. We now rewrite (1) with $\varepsilon = -1$ as

$$p^a = x^2 + (p^b - 1) = x^2 + Du^2 = (x + i\sqrt{D})(x - i\sqrt{D}),$$

and passing to ideals we get $\pi_1^a \pi_2^a = [x + i\sqrt{D}\,u][x - i\sqrt{D}\,u]$. Since x is coprime to p, the ideals $[x + i\sqrt{D}\,u]$ and $[x - i\sqrt{D}\,u]$ are coprime, and by unique factorization for ideals in $\mathcal{O}_{\mathbb{K}}$, there exists $\varepsilon_1 \in \{\pm 1\}$ so that $\pi_1^a = [x + \varepsilon_1\sqrt{D}\,u]$, and $\pi_2^a = [x - \varepsilon_1\sqrt{D}\,u]$. Hence, the order of π_1 in the ideal class group of $\mathbb{K}$ divides a and the same is true for π_2. Let $c := \gcd(a, b)$, and write $a := ca_1$ and $b := cb_1$. Notice that $a_1 \geq 5$. Indeed, this is obviously so when $b_1 \geq 2$, because in this case $a_1 c = a \geq 2b + 1 \geq 2b_1 c + 1 \geq 4c + 1$, therefore $a_1 \geq 5$. When $b_1 = 1$, we have $c = b$, and the fact that we may assume $a_1 \geq 5$ follows from the fact that we have already treated the case $a = 3b$. The ideal π_1^c is now principal; let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be some generator of it. Passing from the ideal equations to elements, it follows that there exist units ζ and ζ' in $\mathcal{O}_{\mathbb{K}}$ so that

$$\alpha^{b_1} = (1 + i\sqrt{D}\,u)\zeta, \qquad \alpha^{a_1} = (x + \varepsilon_1\sqrt{D}\,u)\zeta'. \tag{40}$$

Since $\mathbb{K}$ is complex nonreal, it follows that ζ and ζ' are roots of unity. We also notice that when b_1 is coprime to the order of ζ, we may replace α by $\alpha\zeta^{d_1}$, where d_1 is the multiplicative inverse of b_1 modulo the order of ζ, and with this replacement we may assume that $\zeta = 1$ in (40).

We now distinguish the following cases:

Case 1: $D > 3$. In this case, $\mathbb{K}$ contains only the trivial units ± 1, therefore $\zeta, \zeta' \in \{\pm 1\}$. Writing β for the complex conjugate of α, which is the same as the conjugate in $\mathbb{K}$ of α, and identifying imaginary parts in (40), we get

$$\frac{\alpha^{b_1} - \beta^{b_1}}{\alpha - \beta} = \zeta\,\frac{2i\sqrt{D}\,u}{\alpha - \beta}, \qquad \frac{\alpha^{a_1} - \beta^{a_1}}{\alpha - \beta} = \zeta'\varepsilon_1\,\frac{2i\sqrt{D}\,u}{\alpha - \beta}. \tag{41}$$

Let $(u_k)_{k \geq 0}$ be the Lucas sequence of roots α and β whose general formula is given by

$$u_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{for all } k \geq 0. \tag{42}$$

It is clear that this is indeed a Lucas sequence because $\alpha + \beta$ and $\alpha\beta$ are coprime integers (they are clearly integers because α and β are conjugate algebraic integers, and they are coprime because $[\alpha]$ and $[\beta]$ in $\mathbb{K}$ are powers of π_1 and π_2, respectively), and α/β is not a root of 1. The number u_k is always an integer, and equations (41) show that $u_{a_1} = \pm u_{b_1}$. In particular, every prime divisor of u_{a_1} divides u_{b_1}, and therefore u_{a_1} lacks primitive divisors. Since $a_1 \geq 5$ is odd, by the results from [2], $a_1 \in \{5, 7, 13\}$, and for each of these values of a_1 there are only finitely many possibilities for the pair of roots (α, β), and all these possibilities are listed in Table 1 of [2]. A quick computation shows that none of these exceptional pairs of roots leads to a new solution of (1). In fact, if $a_1 = 5$, then the only possibilities for $p^c = \alpha\beta$ from Table 1 of [2] are $2, 3, 4, 11, 55, 377$; now $2, 4$ are not convenient because they are even, 55, 377 are not convenient because they are not powers of primes, while $c = 1$ and $p \in \{3, 11\}$ simply do not produce new solutions because $p^5 - p^{b_1} + 1$ is never a square for such values of p and $b_1 \in \{1, 2\}$. A similar argument works for $a_1 = 7, 13$.

Case 2: $D = 3$. In this case, we must have $p^b - 1 = 3u^2$. It is known that the equation $y^n = 3v^2 + 1$ has no integer solutions (y, v, n) with $y > 1$ and $n \geq 3$ (see, for example, [5, p. 81]). Thus, $b \leq 2$, and since a is odd, it follows that $c = 1$ and $b = b_1$. All the units in the ring $\mathcal{O}_{\mathbb{K}}$ are of the form $\pm\omega^i$, where $i \in \{0, 1, 2\}$, with ω a primitive root of unity of degree 3. Since $b_1 \leq 2$, it follows that b_1 is coprime to 3, and by the remarks preceding Case 1, we may assume that $\zeta = \pm 1$ in (40). The ring $\mathcal{O}_{\mathbb{K}}$ has integral base $\{1, (1+i\sqrt{3})/2\}$, and therefore we may write $\alpha := (m + in\sqrt{3})/2$ with m and n some integers which are congruent modulo 2. Since $b_1 = 1,\ 2$, formula (40) with $\zeta = 1$ implies that m and n are both even (this is obviously so when $b_1 = 1$, while when $b_1 = 2$ we get $\alpha^2 = (m^2 - 3n^2)/4 + i\sqrt{3}\,mn/2$, and this number is obviously not of the form $\pm(1 + i\sqrt{3}\,u)$ with some integer u when both m and n are odd). This argument shows that we may assume that $\alpha = m_1 + in_1\sqrt{3}$ with some nonzero integers m_1 and n_1 such that m_1 and $3n_1$ are coprime. Hence, α^{a_1} is also of the form $m_2 + n_2 i\sqrt{3}$ with some integers m_2 and n_2. This remark, together with the fact that x is odd and u is even, shows that the unit ζ' appearing in (40) must be ± 1. Indeed, if $\zeta' = \pm\omega^i$ with some $i = 1, 2$, then one can check that $(x + \varepsilon_1)\zeta'$ is of the form $(m_3 + in_3\sqrt{3})/2$ with two odd integers m_3 and n_3.

The above discussion shows that we may assume that $\zeta, \zeta' \in \{\pm 1\}$, and we are therefore in the situation of the preceding case (in fact, none of the exceptional pairs of roots appearing in Table 1 of [2] consists of members of $\mathbb{Q}[i\sqrt{3}]$).

Case 3: $D = 1$. In this case, we have $p^b - 1 = u^2$, and by the result from [8], it follows that $b = 1$. Thus, $c = b_1 = 1$, and we may assume that $\zeta = 1$ in (40). If $\zeta' = \pm 1$, we are in the situation of Case 1, therefore we may assume that $\zeta' = \pm i$. Thus, we have $\alpha = 1 + iu$, $\alpha + \beta = 2$, $\alpha - \beta = 2iu$, and $\alpha^{a_1} = \pm(ix - \varepsilon_1 u)$, therefore $\alpha^{a_1} + \beta^{a_1} = \pm 2u$, and so

$$\frac{\alpha^{2a_1} - \beta^{2a_1}}{\alpha - \beta} = \pm 2u \cdot \frac{\alpha^{a_1} - \beta^{a_1}}{\alpha - \beta},$$

and therefore, with the notation (42), every prime divisor of u_{2a_1} is a prime divisor of either u_{a_1} or $4u^2 = (\alpha-\beta)^2$. Thus, u_{2a_1} is a defective Lucas number with $2a_1 \geq 10$ and whose pair of roots consists of conjugate elements in $\mathbb{Q}[i]$, and by Table 1 of [2], such a Lucas number does not exist.

5. Concluding remarks. Following Szalay [11], it will be of interest to completely solve the equation $x^2 = p^M \pm p^N \pm p^L$ in nonnegative integers x, p, M, N, L with $p > 2$ a prime number. In order to do this, by the results of our paper, it suffices to treat the equations

$$x^2 = p^a \pm p^b - 1, \tag{43}$$

where $a \geq b$. If $b = 0$, we get the equations $x^2 = p^a$ and $x^2 = p^a - 2$, respectively. The first one has the solution $x = p^{a/2}$ when a is even and independently of p, while the only solution of the second equation with $a \geq 2$ is $(x, p, a) = (5, 3, 3)$ (see [9] for a more general statement). It is not known if the second equation above has finitely or infinitely many solutions with $a = 1$, although it is conjectured that there should be infinitely many primes p of the form $x^2 + 2$. When $a = b$, we get the equation $x^2 = -1$ (with no real solution), and $x^2 = 2p^a - 1$, respectively. The only solution with $a \geq 3$ of this last equation is $(x, p, a) = (239, 13, 4)$ (see [4]), and it is not known if this last equation has finitely or infinitely many solutions with $a = 1, 2$. Finally, when $a > b > 0$, the equation

$$x^2 = p^a - p^b - 1$$

has no solutions, because by reducing it modulo p first, we see that $(-1|p) = 1$, therefore $p \equiv 1 \pmod 4$, and now reducing it modulo 4, we get $x^2 \equiv -1 \pmod 4$, which is impossible.

However, we have no idea what to say about the equation

$$x^2 = p^a + p^b - 1,$$

with $a > b > 0$, and a odd, and we leave this last equation to the reader.

Acknowledgements. I would like to thank R. Scott, R. Styer and P. G. Walsh for various useful comments and remarks, and L. Szalay for sending me a copy of [11] before it actually appeared in print. This work was supported in part by grants SEP-CONACYT 37259-E, 37260-E and ANUIES-ECOS M02-M01.

References

[1] M. A. Bennett and C. M. Skinner, *Ternary diophantine equations via Galois representations and modular forms*, preprint, 2002.

[2] Y. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. Reine Angew. Math. 539 (2001), 75–122.

[3] R. D. Carmichael, *On the numerical factors of arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) 15 (1913), 30–70.

[4] J. H. E. Cohn, *Perfect Pell powers*, Glasgow Math. J. 38 (1996), 19–20.

[5] —, *The Diophantine equation* $x^n = Dy^2 + 1$, Acta Arith. 106 (2003), 73–83.

[6] C. Ko, *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica 14 (1965), 457–460.

[7] M. Laurent, M. Mignotte et Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.

[8] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. 9 (1850), 178–181.

[9] F. Luca, *On the equation* $x^2 + 2^a \cdot 3^b = y^n$, Int. J. Math. Math. Sci. 29 (2002), 239–244.

[10] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

[11] L. Szalay, *The equations* $2^N \pm 2^M \pm 2^L = z^2$, Indag. Math. 13 (2002), 131–142.

Mathematical Institute, UNAM
Ap. Postal 61–3 (Xangari), CP 58 089
Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

Received on 25.11.2002
and in revised form on 22.4.2003 (4403)