Functiones et Approximatio
46.1 (2012), 109–116
doi: 10.7169/facm/2012.46.1.8

ON THE DIOPHANTINE EQUATION $2^x = x^2 + y^2 - 2$

Alexandru Gica, Florian Luca

Abstract: In this paper, we show that the only positive integer solutions of the equation $2^x = x^2+y^2-2$ are $(x,y) = (3,1),\ (5,3),\ (7,9)$. We propose also the following conjecture: the equation $2^x = y^2 + z^2(x^2-2)$, where y,z are odd positive integers and x is a positive integer such that x^2-2 is a prime number, has the only solutions $(x,y,z) = (3,1,1),\ (5,3,1),\ (7,9,1),\ (13,3,7)$. The conjecture implies a recent result of Lee [4] which states that if x^2-2 is an odd prime number such that the class number $h(x^2-2)$ of the quadratic field $\mathbb{Q}[\sqrt{x^2-2}]$ is 1, then $x = 3,5,7,13$.

Keywords: diophantine equations, applications of Baker's method.

1. Introduction and Motivation

In this paper, we solve the Diophantine equation

$$2^x = x^2 + y^2 - 2 \tag{1}$$

in positive integers x and y. The result is the following.

Theorem 1. *The only positive integer solutions of equation* (1) *are* $(x,y) = (3,1),\ (5,3),\ (7,9)$.

Before getting to the proof, let us give some motivation for solving this particular Diophantine equation. In [4], Jungyun Lee proved the following conjecture of Mollin and Williams (see Conjecture 5.4.4. on page 176 of [5]).

Theorem 2. *Let $d = n^2 \pm 2$ be a squarefree integer. Then $\mathbb{Q}[\sqrt{d}]$ has class number $h(d) > 1$ if $n > 20$.*

Work by A. G. was partially supported by CNCSIS–UEFISCSU, project number PN II - IDEI, 443, code 1190/2008. F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508. Work on this paper started during the conference NTA 2010 in Debrecen, Hungary, in October 2010. Both authors thank the organizers for the opportunity to attend this event.

2010 Mathematics Subject Classification: primary: 11D61; secondary: 11J70, 11J86

The following is a consequence of the above theorem.

Theorem 3. *Let p be a prime number with the property that $p - a^2$ is a prime number for every even positive integer $a < \sqrt{p}$ and $p - a^2$ is twice times a prime number for every odd positive integer $a < \sqrt{p}$. Then $p = 7, 23, 47, 167$.*

Proof. In [3], the first author analyzed this problem and proved that all prime numbers p which fulfil the above conditions have to be of the form $p = x^2 - 2$ with some odd positive integer x such that every odd prime $q < p$ has the property that p is a quadratic non-residue modulo q. Let us consider now the quadratic field $\mathbb{K} := \mathbb{Q}[\sqrt{p}]$ and let $\mathcal{O}_{\mathbb{K}}$ be its ring of integers. The Minkowski constant for $\mathbb{K}$ is

$$\sqrt{p} = \sqrt{x^2 - 2} < x.$$

Since p is a quadratic non-residue modulo q for all odd primes $q < x$, it follows that $q\mathcal{O}_{\mathbb{K}}$ is a prime ideal of $\mathcal{O}_{\mathbb{K}}$. Since $p \equiv 3 \pmod 4$, we have that $2\mathcal{O}_{\mathbb{K}} = P^2$, where P is a prime ideal with norm 2. But $N(x + \sqrt{p}) = x^2 - p = x^2 - (x^2 - 2) = 2$, so $P = (x + \sqrt{p})\mathcal{O}_{\mathbb{K}}$ is also a principal ideal. Here and in what follows, we use $N_{\mathbb{K}/\mathbb{Q}}$ for the norm map from $\mathbb{K}$ to $\mathbb{Q}$ either at the level of ideals or of elements. Since all prime ideals whose norms are below the Minkowski constant are principal, we deduce that $\mathcal{O}_{\mathbb{K}}$ is a principal ideal domain, so $h(p) = 1$, and now Theorem 2 ensures that $p = 7, 23, 47, 167$. ■

In an attempt to give a proof of Theorem 3 without using Theorem 2, we were led to the following conjecture.

Conjecture 4. *The only solutions of the Diophantine equation $2^x = y^2 + z^2(x^2 - 2)$ in odd positive integers x, y, z such that $x^2 - 2$ is prime number are $(x, y, z) = (3, 1, 1),\ (5, 3, 1),\ (7, 9, 1),\ (13, 3, 7)$.*

Next we show how the truth of Conjecture 4 implies the Theorem 2. Let us suppose that $p = x^2 - 2$ is an odd prime such that $h(p) = 1$. A beautiful result of Hirzebruch and Zagier [7], says that if $p \equiv 3 \pmod 4$ is a prime number such that $h(p) = 1$ and the continued fraction expansion of $\sqrt{p}$ is $[a_0; \{a_1, a_2, \ldots, a_s\}]$, then the class number of the field $\mathbb{L} = \mathbb{Q}[\sqrt{-p}]$ equals

$$\frac{1}{3}(a_s - a_{s-1} + a_{s-2} - \cdots \pm a_1).$$

Since the expansion of $\sqrt{p} = \sqrt{x^2 - 2}$ as continued fraction is

$$\sqrt{x^2 - 2} = [x - 1; \{1, x - 2, 1, 2(x - 1)\}],$$

we get that the class number of $\mathbb{L}$ is

$$h(-p) = \frac{1}{3}[2(x - 1) - 1 + (x - 2) - 1] = x - 2.$$

Observe that $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[(1+\sqrt{-p})/2]$. Since $p = x^2 - 2 \equiv 7 \pmod 8$, we have that $2\mathcal{O}_{\mathbb{K}} = P_1P_2$, where P_1 and P_2 are distinct prime ideals each of norm 2. Since $h(-p) = x-2$, we get that P_1^{x-2} is a principal ideal. Thus,

$$P_1^{x-2} = \left(\frac{y+z\sqrt{-p}}{2}\right)\mathcal{O}_{\mathbb{K}},$$

for some integers y and z of the same parity. If y and z are even, then putting $y = 2y_1$ and $z = 2z_1$ we get

$$P_1^{x-2} = (y_1 + z_1\sqrt{-p})\mathcal{O}_{\mathbb{L}}.$$

Taking norms in the last equality above we obtain $2^{x-2} = y_1^2 + pz_1^2$. Since $x \geqslant 3$, we get that $y_1 \equiv z_1 \pmod 2$. Hence, $P_1P_2 = 2\mathcal{O}_{\mathbb{K}}$ divides $(y_1 + z_1\sqrt{-p})\mathcal{O}_{\mathbb{L}} = P_1^{x-2}$, which is a contradiction. Thus, both y and z are odd and taking norms in the equality

$$P_1^{x-2} = \left(\frac{y+z\sqrt{-p}}{2}\right)\mathcal{O}_{\mathbb{L}},$$

we get $2^{x-2} = (y^2 + pz^2)/4$, which is the same as

$$2^x = y^2 + z^2(x^2 - 2).$$

The truth of Conjecture 4 now would imply that $x = 3, 5, 7, 13$, so $p = 7, 23, 47, 167$, respectively, which is the conclusion of Theorem 3. ∎

In this paper, we solve the equation

$$2^x = y^2 + x^2 - 2.$$

This is the same as the equation of Conjecture 4 for the particular case $z = 1$. We do not use the fact that $x^2 - 2$ is a prime number. Our technique works whenever z takes on a certain fixed value.

2. The proof of Theorem 1

We assume that $x > 1000$ and we shall look at the small cases later. Rewrite equation (1) as

$$2^x - y^2 = x^2 - 2.$$

Observe that the right-hand side is positive. If x is even, then the left-hand side factors as $(2^{x/2} - y)(2^{x/2} + y)$. Hence, we get

$$2^{x/2} \leqslant 2^{x/2} + y \leqslant 2^x - y^2 = x^2 - 2,$$

which is false for $x > 1000$. Thus, x is odd. Equation (1) can be rewritten as

$$\left(2^{(x-1)/2}\sqrt{2} - y\right)\left(2^{(x-1)/2}\sqrt{2} + y\right) = x^2 - 2,$$

so

$$0 < \sqrt{2} - \frac{y}{2^{(x-1)/2}} < \frac{x^2}{2^{(x-1)/2}(2^{(x-1)/2}\sqrt{2}+y)} < \frac{x^2}{2^{x-1}}.$$

Since x is odd, so is y, therefore the fraction $y/2^{(x-1)/2}$ is reduced. A result of Worley [6] (see also Theorem 1 in [2]), asserts that there exist two nonnegative integers r and s with $\max\{r,s\} < 2x^2$ such that

$$(y, 2^{(x-1)/2}) = (rp_m \pm sp_{m-1}, rq_m \pm sq_{m-1})$$

for some positive integer m, where $\{p_m/q_m\}_{m\geqslant 0}$ is the sequence of convergents of $\sqrt{2}$. Since $\sqrt{2} = [1, \{2\}]$, it follows that $q_0 = 1$, $q_1 = 2$ and $q_{m+2} = 2q_{m+1} + q_m$ for all $m \geqslant 0$. This is a binary recurrent sequence whose general term is

$$q_m = \frac{\alpha^{m+1} - \beta^{m+1}}{\alpha - \beta}, \quad \text{for all} \quad m \geqslant 0, \quad \text{where} \quad (\alpha, \beta) := (1+\sqrt{2}, 1-\sqrt{2}).$$

Thus, we get the relation

$$2^{(x-1)/2} = rq_m \pm sq_{m-1} = \gamma\alpha^m + \delta\beta^m, \tag{2}$$

$$\text{where} \quad (\gamma, \delta) := \left(\frac{r\alpha + \varepsilon s}{\alpha - \beta}, \frac{-r\beta - \varepsilon s}{\alpha - \beta}\right), \quad \text{and} \quad \varepsilon \in \{\pm 1\}.$$

Since $1/\beta = -\alpha$, we have that

$$2^{(x-1)/2} = (-1)^m \gamma \beta^m \left(\alpha^{2m} - \eta\right), \tag{3}$$

where

$$\eta := (-1)^{m-1}\frac{\delta}{\gamma} = \pm\left(\frac{r\beta + \varepsilon s}{r\alpha + \varepsilon s}\right).$$

Let $\mathbb{K} := \mathbb{Q}[\sqrt{2}]$, whose ring of integers $\mathcal{O}_{\mathbb{K}}$ is principal. We compute the exponent of the prime $\sqrt{2}$ appearing in the two sides of equation (3). For a number $\eta \in \mathbb{K}$ let $\nu_{\sqrt{2}}(\eta)$ be the exponent with which $\sqrt{2}$ appears in the factorization of η. We have

$$x - 1 = \nu_{\sqrt{2}}(2^{(x-1)/2}) = \nu_{\sqrt{2}}(\gamma) + m\nu_{\sqrt{2}}(\beta) + \nu_{\sqrt{2}}(\Lambda),$$

where

$$\Lambda := \alpha^{2m} - \eta.$$

Next, observe that since r and s are at most $2x^2$, it follows that

$$|N_{\mathbb{K}/\mathbb{Q}}(\gamma)| = \left|\frac{(r\beta + \varepsilon s)(r\alpha + \varepsilon s)}{(\alpha - \beta)^2}\right| = \left|\frac{r^2\alpha\beta + rs\varepsilon(\alpha + \beta) + s^2}{(2\sqrt{2})^2}\right|$$
$$\leqslant \frac{r^2 + 2rs + s^2}{8} \leqslant 2x^4.$$

Since the prime $\sqrt{2}$ is associated to its conjugate, it follows that $\sqrt{2}$ appears with the same exponent in the factorization of δ and of its conjugate, so

$$\nu_{\sqrt{2}}(\gamma) < \frac{\log(2x^4)}{2\log\sqrt{2}} = \frac{4\log x + \log 2}{\log 2} = \frac{4\log x}{\log 2} + 1. \tag{4}$$

Next, $\nu_{\sqrt{2}}(\beta) = 0$ because β is a unit. Hence, we get that

$$x - 2 - \frac{4\log x}{\log 2} \leqslant \nu_{\sqrt{2}}(\Lambda). \tag{5}$$

It remains to find an upper bound for $\nu_{\sqrt{2}}(\Lambda)$. For this, we use Theorem 3 of [1]. In those notations, we take $\alpha_1 := \alpha$, $\alpha_2 := \eta$, $b_1 := 2m$ and $b_2 := 1$. Next, for our situation we have $e = 2$, $f = 1$ and $D = 2$. We compute the logarithmic heights of α_1 and α_2. Clearly,

$$h(\alpha_1) = \frac{1}{2}\log(1+\sqrt{2}) = 0.440687\ldots$$

Next, observe that the minimal polynomial of α_2 over $\mathbb{Q}[X]$ is

$$\left(X - \frac{r\alpha + \varepsilon s}{r\beta + \varepsilon s}\right)\left(X - \frac{r\beta + \varepsilon s}{r\alpha + \varepsilon s}\right) = X^2 - \frac{6r^2 + 4\varepsilon rs + 2s^2}{-r^2 + 2\varepsilon rs + s^2}X + 1,$$

so the minimal polynomial of α_2 over $\mathbb{Z}[X]$ is a divisor of

$$(-r^2 + 2rs + s^2)\left(X - \frac{r\alpha + \varepsilon s}{r\beta + \varepsilon s}\right)\left(X - \frac{r\beta + \varepsilon s}{r\alpha + \varepsilon s}\right) =: a_0(X - \alpha_2^{(1)})(X - \alpha_2^{(2)}).$$

Recall that

$$h(\alpha_2) = \frac{1}{2}\left(\log|a_0| + \sum_{i=1}^{2}\log\left(\max\left\{1, |\alpha_2^{(i)}|\right\}\right)\right).$$

We need an upper bound for $h(\alpha_2)$. Clearly,

$$|a_0| \leqslant r^2 + 2rs + s^2 = (r+s)^2 < (2x^2 + 2x^2)^2 = 16x^4.$$

Furthermore, one of $\alpha_2^{(1)}$ and $\alpha_2^{(2)}$ is subunitary, and the absolute value of their sum is

$$|\alpha_2^{(1)} + \alpha_2^{(2)}| = \left|\frac{6r^2 + 4\varepsilon rs + 2s^2}{-r^2 + 2\varepsilon rs + s^2}\right| \leqslant 6r^2 + 4rs + 2s^2 \leqslant 48x^4. \tag{6}$$

We thus get immediately that

$$\begin{aligned} h(\alpha_2) &\leqslant \frac{1}{2}\left(\log(16x^4) + \log(48x^4 + 1)\right) \\ &= \frac{1}{2}\left(\log(16) + \log(48) + 8\log x + \log\left(1 + \frac{1}{48x^4}\right)\right) \\ &< 3.5 + 4\log x. \end{aligned}$$

We now choose parameters A_1 and A_2 such that

$$\log A_i \geqslant \max\left\{h(\alpha_i), \frac{\log p}{D}\right\} = \max\left\{h(\alpha_i), \frac{\log 2}{2}\right\}, \qquad \text{for} \quad i = 1, 2.$$

So, we can take $\log A_1 := 0.45$ and $\log A_2 := 3.5 + 4\log x$. Next, we take

$$b := \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1} = \frac{2m}{2(3.5+4\log x)} + \frac{1}{0.9}. \tag{7}$$

We need a bound on m versus x. We use equation (2). Since $\sqrt{2} = [1, \{2\}]$, it follows from the properties of the convergents to α, that the inequality

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{4q^2} \qquad \text{holds for all rational numbers} \quad \frac{p}{q}.$$

Hence,

$$|\gamma| = \left(\frac{r}{\alpha-\beta}\right)\left|\alpha - \left(\frac{-\varepsilon s}{r}\right)\right| > \frac{1}{8\sqrt{2}r} > \frac{1}{16\sqrt{2}x^2} > \frac{1}{23x^2}.$$

The above inequality together with (2) leads to

$$2^{(x-1)/2} \geqslant |\gamma|\alpha^m - |\delta||\beta|^m \geqslant \frac{\alpha^m}{23x^2} - x^2,$$

where we used the fact that

$$|\delta| = \left|\frac{r\beta + \varepsilon s}{\alpha - \beta}\right| \leqslant \frac{r|\beta| + s}{2\sqrt{2}} < \frac{2x^2(|\beta|+1)}{2\sqrt{2}} = x^2.$$

So,

$$\alpha^m < 23x^2(2^{(x-1)/2} + x^2). \tag{8}$$

The right–hand side in estimate (8) above is $< \alpha^{0.8x}$ for all $x > 1000$. Hence,

$$2m < 1.6x. \tag{9}$$

Combining this with (7), we get that

$$b < \frac{1.6x}{7 + 8\log x} + \frac{10}{9} \qquad \text{for} \quad x > 1000. \tag{10}$$

Now Theorem 3 in [1] tells us that if α_1 and α_2 are multiplicatively independent, then

$$\nu_{\sqrt{2}}(\Lambda) \leqslant \frac{24pgD^4}{(p-1)(\log p)^4}\left(\max\left\{\log b + \log\log p + 0.4, \frac{10\log p}{D}, 10\right\}\right)^2$$
$$\times \log A_1 \log A_2.$$

Observe that

$$\log b + \log\log p + 0.4 < \log\left(e^{0.4}(\log 2)\left(\frac{1.6x}{7+8\log x} + \frac{10}{9}\right)\right)$$
$$< \log\left(x\left(\frac{1.7}{7+8\log x} + \frac{1.15}{x}\right)\right) < \log\left(\frac{x}{4\log x}\right),$$

where the last inequality above holds because the inequality

$$\frac{1.7}{7+8\log x} + \frac{1.15}{x} < \frac{1}{4\log x} \qquad \text{holds for all} \quad x > 1000.$$

So, we get using also inequality (5), that

$$x - 2 - \frac{4\log x}{\log 2} \leqslant \nu_{\sqrt{2}}(\Lambda) \leqslant 24 \cdot 2 \cdot (\log 2)^{-4} \cdot 2^4 \cdot 0.45 \cdot (3.5 + 4\log x)$$
$$\times \left(\max\left\{\log\left(\frac{x}{4\log x}\right), 10\right\}\right)^2.$$

When the maximum on the right above is 10, we get that $x/(4\log x) < e^{10}$, so $x < 2 \times 10^6$, while when the maximum on the right above is $\log(x/(4\log x))$, we get that $x < 4 \times 10^6$. Hence, at any rate $x < 4 \times 10^6$.

All this was when η and α were multiplicatively independent. Otherwise, since α is the fundamental unit of $\mathcal{O}_{\mathbb{K}}$, it follows that $\eta = \pm\alpha^t$ for some integer t. By inequality (6), we get that

$$|t| \leqslant \frac{\log(48x^4+1)}{\log\alpha} = \frac{1}{\log\alpha}\left(\log 48 + 4\log x + \log\left(1 + \frac{1}{48x^4}\right)\right)$$
$$< 1.2(3.9 + 4\log x) < 5 + 5\log x. \tag{11}$$

Thus, $\eta^{-1}\Lambda = \pm\alpha^{2m+t} - 1$, which is a divisor of

$$\alpha^{8m+4t} - 1 = \alpha^{4m+2t}(\alpha^{4m+2t} - \beta^{4m+2t}) = 2\sqrt{2}\alpha^{4m+2t}q_{4m+2t+1}.$$

Comparing this with inequality (5), we get that the exponent of $\sqrt{2}$ in $q_{4m+2t+1}$ exceeds

$$x - 5 - \frac{4\log x}{\log 2}.$$

However, $q_{4m+2t+1}$ is an integer. Hence, the exponent of 2 in $q_{4m+2t+1}$ is

$$\geqslant \frac{x-5}{2} - \frac{2\log x}{\log 2}.$$

It is an elementary exercise to prove that the exponent of 2 in q_n is the exponent of 2 in $n+1$ (Hint: Use induction over the exponent of 2 in the factorization of $n+1$ together with the fact that for odd n one has

$$q_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = \frac{\alpha^{(n+1)/2} - \beta^{(n+1)/2}}{\alpha - \beta}(\alpha^{(n+1)/2} + \beta^{(n+1)/2})$$
$$= q_{(n-1)/2}(\alpha^{(n+1)/2} + \beta^{(n+1)/2}),$$

and $\alpha^m + \beta^m$ is an integer which is congruent to 2 modulo 4 for all nonnegative integers m.) Hence, we get that

$$\frac{x-5}{2} - \frac{2\log x}{\log 2} \leqslant 1 + \frac{\log(2m+t+1)}{\log 2}.$$

Using inequalities (9) and (11), we arrive at

$$\frac{x-5}{2} - \frac{2\log x}{\log 2} \leqslant 1 + \frac{\log(1.6x+6+5\log x)}{\log 2},$$

yielding $x < 42$, which is much better than just $x < 4 \times 10^6$.

Thus, we always have $x < 4 \times 10^6$. For these remaining values of x, we checked with Mathematica that for all $x \leqslant 4 \times 10^6$ except $x \in \{3, 5, 7\}$, there exists an odd prime p among the first 50 odd primes such that the Legendre symbol $\left(\frac{2^x - x^2 + 2}{p}\right)$ evaluates to -1. Hence, $2^x - x^2 + 2$ cannot be a perfect square for $x \leqslant 4 \times 10^6$ except for the three values $x = 3, 5, 7$. This computation took a few minutes. This completes the proof of the theorem.

References

[1] Y. Bugeaud and M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. of Number Theory **61** (1996), 311–342.

[2] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[3] A. Gica, *An additive problem*, An. Univ. Buc. Mat. **53** (2004), 229–234.

[4] J. Lee, *The complete determination of wide Richaud-Degert types which are not 5 modulo 8 with class number one*, Acta Arith. **140** (2009), 1–29.

[5] R. A. Mollin, *Quadratics*, CRC Press, 1996.

[6] R. T. Worley, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. **31** (1981), 202–206.

[7] D. Zagier, *Nombres de classes et fractions continues*, Astérisque **24-25** (1975), 81–97.

Addresses: Alexandru Gica: Department of Mathematics, University of Bucharest, Str. Academiei nr.14, sector 1, C.P. 010014, Bucuresti, Romania;
Florian Luca: Centro de Ciencias Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México.

E-mail: alexgica@yahoo.com, fluca@matmor.unam.mx

Received: 9 December 2010