On the Diophantine Equation $x^2 + C = 2^r y^n$

Szabolcs Tengely
University of Debrecen
Supported by OTKA PD75264 and
János Bolyai Research Scholarship
of the Hungarian Academy of Sciences

19th Czech and Slovak International Conference
on Number Theory

31st August-4th September, 2009

Outline

In this lecture we report on two results:

$$x^2 + C = 2y^n,$$

joint work with F. S. Abu Muriefah, F. Luca and S. Siksek, and

$$x^2 + C = 4y^n,$$

joint work with F. Luca and A. Togbé.

Earlier results

- $x^m = y^2 + 1$: Lebesgue (1850).
- $Cx^2 + D = y^n$: Ljunggren (1964).
- $x^2 = y^n + 1$: Ko (1965).
- $Cx^2 + D = 2y^n$: Ljunggren (1966).
- $y^m = P(x)$: general result by Schinzel and Tijdeman $\Rightarrow$ for fixed A, B, C there are only finitely many solutions $x, y, n > 2$ of $Ax^2 + B = Cy^n$, (1976).
- $x^2 + C = y^n$: Cohn, 81 values of C in the range $1 \leq C \leq 100$, (1993, 2003).
- $x^2 + 7 = y^n$: Cremona and Siksek, for any unknown solution (x, y, n) one has $10^8 < n < 6.6 \times 10^{15}$, (2003).
- $x^2 + D = y^n, 1 \leq D \leq 100$: Bugeaud, Mignotte and Siksek, complete resolution by means of Baker's method and modular approach (2006).

- $x^2 + 2^a 3^b = y^p$ Luca (2002).
- $x^2 + p^{2k+1} = 4y^n$ Arif and Al-Ali (2002).
- $x^2 + 5^{2k} = y^n$ Muriefah (2006).
- $x^2 + q^{2m} = 2y^p$: Tengely, finiteness result, complete solution of the case $q = 3$, (2007).
- $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$: Goins, Luca and Togbé (2008).
- $x^2 + p^{2k} = y^n$: Bérczes and Pink, all solutions for $2 \leq p < 100$, prime, (2008).

Theorem (Tengely). *There are only finitely many solutions* (x, y, m, q, p) *of* $x^2 + q^{2m} = 2y^p$ *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not a sum of two consecutive squares,* $m \in \mathbb{N}$ *and* $p > 3, q$ *are odd primes.*

Theorem (Tengely). *There are only finitely many solutions* (x, y, m, q, p) *of* $x^2 + q^{2m} = 2y^p$ *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not a sum of two consecutive squares,* $m \in \mathbb{N}$ *and* $p > 3, q$ *are odd primes.*

The question of finiteness if y is a sum of two consecutive squares is interesting. The following examples, all for $m = 1$, show that very large solutions exist.

y	p	q
5	5	79
5	7	307
5	13	42641
5	29	1811852719
5	97	229935753703632302559452847176639 9

We have

$$x = \Re((1+i)(u+iv)^p) =: F_p(u,v),$$
$$q^m = \Im((1+i)(u+iv)^p) =: G_p(u,v).$$

Let $H_p(u,v) = \frac{G_p(u,v)}{u+\delta_4 v}$.

$$u + \delta_4 v = q^k, \qquad (1)$$
$$H_p(u,v) = q^{m-k},$$

$$u + \delta_4 v = -q^k, \qquad (2)$$
$$H_p(u,v) = -q^{m-k},$$

Remark. Schinzel's Hypothesis H says that if $P_1(X), \ldots, P_r(X) \in \mathbb{Z}[X]$ are irreducible polynomials with positive leading coefficients such that no integer $l > 1$ divides $P_i(x)$ for all integers x for some $i \in \{1, \ldots, k\}$, then there exist infinitely many positive integers x such that $P_1(x), \ldots, P_r(x)$ are simultaneously prime. Since $\pm H_p(\pm 1 - \delta_4 v, v)$ is irreducible having constant term ± 1, the Hypothesis implies that in case of $k = 0, m = 1$ there are infinitely many solutions of (1) and (2). Hence there are infinitely many solutions of $x^2 + q^2 = 2y^p$.

Lehmer Sequences

A *Lehmer pair* is a pair (α, β) of algebraic integers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a Lehmer pair (α, β), the corresponding *Lehmer sequence* $\{u_n\}$ is given by

$$u_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even.} \end{cases}$$

A prime q is called a *primitive divisor* of the term u_n if q divides u_n but q does not divide $(\alpha^2 - \beta^2)^2 u_1 \dots u_{n-1}$.

The equation $x^2 + C = 2y^p$

Theorem (Abu Muriefah, Luca, Siksek, Tengely). *Let C be a positive integer satisfying $C \equiv 1 \pmod 4$, and write $C = cd^2$, where c is square-free. Suppose that (x, y) is a solution to the equation*

$$x^2 + C = 2y^p, \qquad x,\ y \in \mathbb{Z}^+, \quad \gcd(x, y) = 1,$$

where $p \geq 5$ is a prime. Then either

(i) $x = y = C = 1$, *or*

(ii) p *divides the class number of the quadratic field* $\mathbb{Q}(\sqrt{-c})$, *or*

(iii) $p = 5$ *and* $(C, x, y) = (9, 79, 5), (125, 19, 3), (125, 183, 7), (2125, 21417, 47)$, *or*

(iv) $p \mid (q - (-c|q))$, *where q is some odd prime such that $q \mid d$ and $q \nmid c$. Here $(c|q)$ denotes the Legendre symbol of the integer c with respect to the prime q.*

Sketch of the proof

About the proof: $x^2 + cd^2 = 2y^p$, assume that $(cd^2, x, y) \neq (1, 1, 1)$ and $p \nmid$ class number of $\mathbb{Q}(\sqrt{-c})$. Here $\mathcal{O} = \mathbb{Z}[\sqrt{-c}]$ and $(2) = \mathfrak{q}^2$. We obtain that

$$2^{(p-1)/2}(x + d\sqrt{-c})\mathcal{O} = (\mathfrak{q}\mathfrak{a})^p.$$

Hence $2^{(p-1)/2}(x + d\sqrt{-c}) = (U + V\sqrt{-c})^p$ for some integers U, V. In conclusion,

$$\frac{x + d\sqrt{-c}}{\sqrt{2}} = \left(\frac{U + V\sqrt{-c}}{\sqrt{2}}\right)^p.$$

$$\alpha = \frac{U + V\sqrt{-c}}{\sqrt{2}}, \qquad \beta = \frac{U - V\sqrt{-c}}{\sqrt{2}}.$$

Then (α, β) is a Lehmer pair.

We note that

$$\alpha^p - \beta^p = d\sqrt{-2c}, \qquad \alpha - \beta = V\sqrt{-2c}.$$

Thus, $V \mid d$ and $u_p \mid d/V$. We have that u_p has a primitive divisor unless $p = 5$ and (c, U^2, V^2) is one of the possibilities listed in the theorem. So we may assume that u_p has a primitive divisor q. Clearly, $q \mid d$, but by the definition of the primitive divisor, $q \nmid (\alpha^2 - \beta^2)^2$ and so, in particular, $q \nmid c$. Let

$$\gamma = U + V\sqrt{-c}, \qquad \delta = U - V\sqrt{-c}.$$

Write $v_n = (\gamma^n - \delta^n)/(\gamma - \delta)$. We note that $q \mid v_p$ but $q \nmid (\gamma - \delta)\gamma\delta$. After checking that $q \mid v_{q-(-c|q)}$ we get that p divides $q - (-c|q)$, (a result by Bugeaud, Luca, Mignotte and Siksek).

Applications

Theorem (Abu Muriefah, Luca, Siksek, Tengely). *The only solutions to the equation* $x^2 + C = 2y^n$ *with* x, y *coprime integers,* $n \geq 3$, *and* $C \equiv 1 \pmod 4$, $1 \leq C < 100$ *are*

$$1^2 + 1 = 2 \cdot 1^n, \quad 79^2 + 9 = 2 \cdot 5^5, \quad 5^2 + 29 = 2 \cdot 3^3,$$
$$117^2 + 29 = 2 \cdot 19^3, \quad 993^2 + 29 = 2 \cdot 79^3, \quad 11^2 + 41 = 2 \cdot 3^4,$$
$$69^2 + 41 = 2 \cdot 7^4, \quad 171^2 + 41 = 2 \cdot 11^4, \quad 1^2 + 53 = 2 \cdot 3^3,$$
$$25^2 + 61 = 2 \cdot 7^3, \quad 51^2 + 61 = 2 \cdot 11^3, \quad 37^2 + 89 = 2 \cdot 9^3.$$

About the Proof. Previous Theorem implies that $(C, x, y) \in \{(1, 1, 1), (9, 79, 5)\}$ or $p \in \{2, 3\}$. It remains to solve the equations $x^2 + C = 2y^3$ and $x^2 + C = 2y^4$ for $C \equiv 1 \pmod 4$, $1 \leq C < 100$.

Theorem (ALST). *The only solutions to the equation*

$$x^2 + 17^{a_1} = 2y^n, \qquad a_1 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 17^0 = 2 \cdot 1^n, \quad 239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.$$

The only solutions to the equation

$$x^2 + 5^{a_1} 13^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 5^0 \cdot 13^0 = 2 \cdot 1^n, \quad 9^2 + 5^0 \cdot 13^2 = 2 \cdot 5^3, \quad 7^2 + 5^1 \cdot 13^0 = 2 \cdot 3^3,$$
$$99^2 + 5^2 \cdot 13^0 = 2 \cdot 17^3, \quad 19^2 + 5^2 \cdot 13^1 = 2 \cdot 7^3,$$
$$79137^2 + 5^2 \cdot 13^3 = 2 \cdot 1463^3, \quad 253^2 + 5^2 \cdot 13^4 = 2 \cdot 73^3,$$
$$188000497^2 + 5^8 \cdot 13^4 = 2 \cdot 260473^3, \quad 239^2 + 5^0 \cdot 13^0 = 2 \cdot 13^4.$$

Theorem (ALST). *The only solutions to the equation*

$$x^2 + 3^{a_1}11^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 3^0 \cdot 11^0 = 2 \cdot 1^n, \quad 351^2 + 3^0 \cdot 11^4 = 2 \cdot 41^3,$$
$$13^2 + 3^4 \cdot 11^0 = 2 \cdot 5^3, \quad 5^2 + 3^4 \cdot 11^2 = 2 \cdot 17^3,$$
$$27607^2 + 3^4 \cdot 11^2 = 2 \cdot 725^3, \quad 545^2 + 3^6 \cdot 11^0 = 2 \cdot 53^3,$$
$$679^2 + 3^6 \cdot 11^2 = 2 \cdot 65^3, \quad 1093^2 + 3^8 \cdot 11^4 = 2 \cdot 365^3,$$
$$410639^2 + 3^{10} \cdot 11^2 = 2 \cdot 4385^3, \quad 239^2 + 3^0 \cdot 11^0 = 2 \cdot 13^4,$$
$$79^2 + 3^2 \cdot 11^0 = 2 \cdot 5^5.$$

The equation $x^2 + C = 4y^p$

Theorem (Luca, Tengely, Togbé). *The only integer solutions* (C, n, x, y) *of the Diophantine equation*

$$x^2 + C = 4y^n, \quad x, y \geq 1, \quad \gcd(x, y) = 1,$$
$$n \geq 3, \quad C \equiv 3 \mod 4, \quad 1 \leq C \leq 100$$

are given in the following table:

$(3, n, 1, 1)$	$(3, 3, 37, 7)$	$(7, 3, 5, 2)$	$(7, 5, 11, 2)$
$(7, 13, 181, 2)$	$(11, 5, 31, 3)$	$(15, 4, 7, 2)$	$(19, 7, 559, 5)$
$(23, 3, 3, 2)$	$(23, 3, 29, 6)$	$(23, 3, 45, 8)$	$(23, 3, 83, 12)$
$(23, 3, 7251, 236)$	$(23, 9, 45, 2)$	$(31, 3, 1, 2)$	$(31, 3, 15, 4)$
$(31, 3, 63, 10)$	$(31, 3, 3313, 140)$	$(31, 6, 15, 2)$	$(35, 4, 17, 3)$
$(39, 4, 5, 2)$	$(47, 5, 9, 2)$	$(55, 4, 3, 2)$	$(59, 3, 7, 3)$
$(59, 3, 21, 5)$	$(59, 3, 525, 41)$	$(59, 3, 28735, 591)$	$(63, 4, 1, 2)$
$(63, 4, 31, 4)$	$(63, 8, 31, 2)$	$(71, 3, 235, 24)$	$(71, 7, 21, 2)$
$(79, 3, 265, 26)$	$(79, 5, 7, 2)$	$(83, 3, 5, 3)$	$(83, 3, 3785, 153)$
$(87, 3, 13, 4)$	$(87, 3, 1651, 88)$	$(87, 6, 13, 2)$	$(99, 4, 49, 5)$

Sketch of the proof

About the proof: the cases $p = 2, 3$ can be reduced to elliptic curves. The class numbers of the related number fields are 1,2,3,4,6,8 for $1 \leq C \leq 100$, except for $C = 47, 79$ for which $h = 5$, and $C = 71$ for which $h = 7$, respectively.

$$x^2 + 47 = 4y^5, \qquad x^2 + 79 = 4y^5, \qquad x^2 + 71 = 4y^7.$$

One can reduce the above equations to Thue equations, e.g. when $C = 71$ and $p = 7$ we have:

$$\pm 16384 = u^7 - 147u^6v - 1491u^5v^2 + 52185u^4v^3 + 176435u^3v^4 \\ -2223081u^2v^5 - 2505377uv^6 + 7516131v^7.$$

PARI/GP $\rightarrow (u, v) = (\pm 4, 0) \Rightarrow (x, y) = (21, 2)$.

$$\pm 2097152 = 21u^7 - 1295u^6v - 31311u^5v^2 + 459725u^4v^3$$
$$+3705135u^3v^4 - 19584285u^2v^5 - 52612917uv^6 + 66213535v^7.$$

PARI/GP $\rightarrow$ no solutions.

$$\pm 268435456 = 313u^7 - 8379u^6v - 466683u^5v^2 + 2974545u^4v^3$$
$$+55224155u^3v^4 - 126715617u^2v^5 - 784183001uv^6 + 428419467v^7.$$

These Thue equations are all impossible modulo 43.

Applications

Theorem (LTT). *The only integer solutions of the Diophantine equation*

$$x^2+7^a\cdot 11^b = 4y^n, \quad x,y\geq 1, \quad \gcd(x,y)=1, \quad n\geq 3, \quad a,b\geq 0$$

are:

$$5^2+7^1\cdot 11^0 = 4\cdot 2^3, \qquad 11^2+7^1\cdot 11^0 = 4\cdot 2^5,$$
$$31^2+7^0\cdot 11^1 = 4\cdot 3^5, \qquad 57^2+7^1\cdot 11^2 = 4\cdot 4^5,$$
$$13^2+7^3\cdot 11^0 = 4\cdot 2^7, \qquad 57^2+7^1\cdot 11^2 = 4\cdot 2^{10}$$
$$181^2+7^1\cdot 11^0 = 4\cdot 2^{13}.$$

Theorem (LTT). *The only integer solutions of the Diophantine equation*

$$x^2+7^a\cdot 13^b = 4y^n, \quad x,y\geq 1, \quad \gcd(x,y)=1, \quad n\geq 3, \quad a,b\geq 0$$

are:

$$5^2+7^1\cdot 13^0 = 4\cdot 2^3, \qquad 5371655^2+7^3\cdot 13^2 = 4\cdot 19322^3,$$
$$11^2+7^1\cdot 13^0 = 4\cdot 2^5, \qquad 13^2+7^3\cdot 13^0 = 4\cdot 2^7,$$
$$87^2+7^3\cdot 13^2 = 4\cdot 4^7, \qquad 181^2+7^1\cdot 13^0 = 4\cdot 2^{13},$$
$$87^2+7^3\cdot 13^2 = 4\cdot 2^{14}.$$