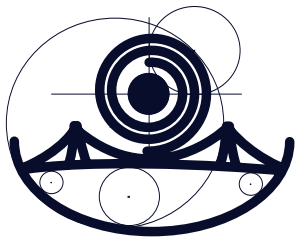
A Pellian equation with primes and its applications

Ivan Soldo

Department of Mathematics, University of Osijek, Croatia



Representation Theory XVI,
June 23-29, 2019, Inter-University Centre Dubrovnik, Croatia

A. DUJELLA, M. JUKIĆ BOKUN, I. SOLDO, *A Pellian equation with primes and applications to $D(-1)$-quadruples*, Bull. Malays. Math. Sci. Soc., to appear.

Let p be an odd prime and k a non-negative integer. We consider the Pellian equation

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1}, \quad l \in \{0, 1, \ldots, k\}. \tag{1}$$

The main result of this section is the following theorem:

THEOREM 1.
The equation (1) *has no solutions in positive integers x and y.*

PROOF: The proof is organized through the three cases.

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1} \quad (1)$$

Case 1. Let $2l + 1 \leq k + 1$, i.e. $l \leq \frac{k}{2}$.

Y. FUJITA, *The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$, with $|k|$ prime*, Glas. Mat. Ser. III **41** (2006), 205–216.

LEMMA 1 [Lemma 2, F.].
Let N and K be integers with $1 < |N| \leq K$. Then the Pellian equation

$$X^2 - (K^2 + 1)Y^2 = N$$

has no primitive solution.

The solution (X_0, Y_0) is called primitive if $\gcd(X_0, Y_0) = 1$.

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1} \quad (1)$$

By Lemma 1, we know that the equation (1) has no primitive solutions. Assume that there exists a non-primitive solution (x, y). Then $p|x$ and $p|y$, so there exist $0 < i \leq l, x_1, y_1 \geq 0$, $\gcd(x_1, y_1) = 1$ such that $x = p^i x_1, y = p^i y_1$. After dividing equation (1) by p^{2i}, we obtain

$$x_1^2 - (p^{2k+2} + 1)y_1^2 = -p^{2l-2i+1}, \quad 0 < 2l - 2i + 1 \leq k + 1.$$

But such x_1, y_1 do not exist according to Lemma 1, so we obtained a contradiction.

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1} \quad (1)$$

Case 2. Let $2l + 1 = 2k + 1$, i.e. $l = k$.

Firstly we proved

LEMMA 2
If (x, y) is a solution of the equation

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2k+1}, \quad (2)$$

and $y \geq p^{\frac{2k+1}{2}}$, then the inequality

$$\sqrt{p^{2k+2} + 1} + \frac{x}{y} > 2p^{k+1}$$

holds.

If we suppose that there exists a solution (x, y) of the equation (1) such that $y \geq p^{\frac{2k+1}{2}}$, then by applying Lemma 2 we obtained

$$|\sqrt{p^{2k+2}+1} - \frac{x}{y}| < \frac{p^k}{2y^2}. \tag{3}$$

Assume that $x = p^t x_1, y = p^t y_1$, where t, x_1, y_1 are non-negative integers and $\gcd(x_1, y_1) = 1$. Now the equation (1) is equivalent to

$$x_1^2 - (p^{2k+2}+1)y_1^2 = -p^{2k-2t+1}. \tag{4}$$

Since $y \geq y_1$, from (3) we obtain

$$|\sqrt{p^{2k+2}+1} - \frac{x_1}{y_1}| < \frac{p^k}{2y_1^2}.$$

R. T. WORLEY, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. Ser. A **31** (1981), 202–206.

THEOREM 2 [Theorem, W.].
Let α be a real number and let a and b be coprime non-zero integers, satisfying the inequality

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

where c is a positive real number. Then $(a, b) = (rp_{m+1} \pm up_m, rq_{m+1} \pm uq_m)$, for some $m \geq -1$ and non-negative integers r and u such that $ru < 2c$. Here p_m/q_m denotes the m-th convergent of continued fraction expansion od α.

Now, Theorem 2 implies that

$$(x_1, y_1) = (rp_{m+1} \pm up_m, rq_{m+1} \pm uq_m), \tag{5}$$

for some $m \geq -1$ and non-negative integers r and u such that

$$ru < p^k. \tag{6}$$

Since x_1 and y_1 are coprime, we have $\gcd(r, u) = 1$.
The terms p_m/q_m are convergents of the continued fraction expansion of $\sqrt{p^{2k+2} + 1}$.

A. DUJELLA, B. JADRIJEVIĆ, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

LEMMA 3 [Lemma 2, D., J.]

Let α, β be positive integers such that $\alpha\beta$ is not a perfect square, and let p_n/q_n denotes the n-th convergent of continued fraction expansion of $\sqrt{\frac{\alpha}{\beta}}$. Let the sequences (s_n) and (t_n) arises from continued fraction expression of the quadratic irrational $\frac{\sqrt{\alpha\beta}}{\beta}$. Then

$$\alpha(rq_{n+1}+uq_n)^2-\beta(rp_{n+1}+up_n)^2=(-1)^n(u^2t_{n+1}+2rus_{n+2}-r^2t_{n+2}),$$

for any real numbers r, u.

In our case

$$\sqrt{p^{2k+2}+1} = [p^{k+1}, \overline{2p^{k+1}}],$$

the period of that continued fraction expansion (and also of the corresponding sequences (s_n) and (t_n)) is equal to 1, according to Lemma 3, we have to consider only the case $m = 0$. We obtain

$$(p^{2k+2}+1)(rq_1 \pm uq_0)^2 - (rp_1 \pm up_0)^2 = u^2 - r^2 \pm 2rup^{k+1}. \quad (7)$$

Therefore we have to study the solvability of the equation

$$u^2 - r^2 \pm 2rup^{k+1} = p^{2k-2t+1}. \quad (8)$$

We proved that such r, u does not exists.

It remains to consider the case $y < p^{\frac{2k+1}{2}}$. Assume that there exists a solution of the equation (1) with this property. In that case we can generate increasing sequence of infinitely many solutions of the equation (1). Therefore, a solution (x, y) such that $y \geq p^{\frac{2k+1}{2}}$ will appear. This contradicts with the first part of the proof of this case.

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1} \quad (1)$$

Case 3. Let $k + 1 < 2l + 1 < 2k + 1$, i.e. $\frac{k}{2} < l < k$.

In this case, if we suppose that the equation (1) has a solution, then multiplying that solution by p^{k-l} we obtain the solution of the equation

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2k+1},$$

which is not solvable by Case 2. That is the contradiction, and this completes the proof of Theorem 1.

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1} \quad (1)$$

PROPOSITION 1.
Let $p = 2$.

(i) If $k \equiv 0 \pmod 2$, then the equation (1) has no solutions.

(ii) If $k \equiv 1 \pmod 2$, then in case of $l > \frac{k}{2}$ the equation (1) has a solution

$$(x, y) = (2^{\frac{2l-k-1}{2}}(2^{k+1} - 1), 2^{\frac{2l-k-1}{2}}),$$

and in case of $l \leq \frac{k}{2}$ it has no solutions.

PROOF: (i) The equation (1) is not solvable modulo 5.
(ii) If $l \leq \frac{k}{2}$, then $2l + 1 \leq k + 1$ and we can proceed as in Case 1 of Theorem 1 and conclude that the equation (1) has no solutions.

DEFINITION 1.
Let n be a non-zero element of a commutative ring R. A Diophantine m-tuple with the property $D(n)$, or simply a $D(n)$-m-tuple, is a set of m non-zero elements of R such that if a, b are any two distinct elements from this set, then $ab + n = k^2$, for some element k in R.

- Fermat set $\{1, 3, 8, 120\}$, i.e., $D(1)$-quadruple in integers;
- the case of $n = -1$: it is conjectured that $D(-1)$-quadruples do not exist in integers;
- Dujella, Filipin and Fuchs: there are at most finitely many $D(-1)$-quadruples; an upper bound for their number was 10^{903};
- Filipin, Fujita, Bonciocat, Cipu, Mignotte, Elsholtz;
- At present, the best known bound for the number of $D(-1)$-quadruples is $3.677 \cdot 10^{58}$ due to Lapkova.

I. SOLDO, *$D(-1)$-triples of the form $\{1, b, c\}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$*, Bull. Malays. Math. Sci. Soc. **39** (2016), 1201-–1224.

THEOREM 3 [Theorem 2.2, S.]

Let $t > 0$ and $\{1, b, c\}$ be $D(-1)$-triple in the ring $\mathbb{Z}[\sqrt{-t}]$.

(i) *If b is a prime, then $c \in \mathbb{Z}$.*

(ii) *If $b = 2p^k$, where p is a prime and $k \in \mathbb{N}$, then $c \in \mathbb{Z}$.*

REMARK 1.
In the proof of Theorem 3, it was shown that for every t there exists such $c > 0$, while the case $c < 0$ is possible only if $t|b-1$ and the equation

$$x^2 - by^2 = \frac{1-b}{t} \tag{9}$$

has an integer solution.

- $b = 2p^k, k \in \mathbb{N}$, where p be an odd prime
- $D(-1)$-triples of the form $\{1, b, c\}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.
- Since $b - 1 = 2p^k - 1$ has to be a square, to reduce the number of t's, we consider the equation of the form

$$2p^k - 1 = q^{2j}, \quad j > 0, \tag{10}$$

where q is an odd prime.

A. KHOSRAVI, B. KHOSRAVI, *A new characterization of some alternating and symmetric groups (II)*, Houston J. Math. **30** (2004), 953–967.

$$2p^k - 1 = q^{2j}, \quad j > 0 \qquad (10)$$

- $(k, j) = (2, 1)$,
  $(p, q) \in \{(5, 7), (29, 41), (44560482149, 63018038201),$
  $(1355877461004671178070 1, 1917500294268803292859 9)\}$
- $(k, j) = (4, 1)$, $(p, q) = (13, 239)$.
- $k = 1, 2, 4$, yields $2p^k = q^{2^l} + 1, l > 0$.

A. Filipin, Y. Fujita, M. Mignotte

The non-extendibility of some parametric families of $D(-1)$-triples, Q. J. Math. **63**(2012), 605–621.

Lemma 4 [Corollary 1.3., F., F., M.].

Let r be a positive integer and let $b = r^2 + 1$. Assume that $b = p$ or $b = 2p^k$, for an odd prime p and a positive integer k. Then the $D(-1)$-pair $\{1, b\}$ cannot be extended to $D(-1)$-quadruple.

THEOREM 4
If p is an odd prime and k, t positive integers with $t \equiv 0 \pmod 2$, then there does not exists a $D(-1)$-quadruple of the form $\{1, 2p^k, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$.

PROOF: Let $t \equiv 0 \pmod 2$. We have that $t \nmid 2p^k - 1$. Therefore, if we suppose that $\{1, 2p^k, c, d\}$ is a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$, then according to Remark 1 we obtain $c, d \in \mathbb{N}$. This means that there exist integers x_1, y_1, u_1, v_1, w_1, such that

$$c - 1 = x_1^2, d - 1 = y_1^2, 2p^k c - 1 = u_1^2, 2p^k d - 1 = v_1^2, cd - 1 = w_1^2,$$

or at least one of $c - 1, d - 1, 2p^k c - 1, 2p^k d - 1, cd - 1$ is equal to $-tw_2^2$, for an integer w_2.
The first possibility leads to contradiction with Lemma 4, i.e., a $D(-1)$-pair $\{1, 2p^k\}$, cannot be extended to a $D(-1)$-quadruple in integers, while the second one contradicts to $c, d \in \mathbb{N}$.

The case of $t \equiv 1 \pmod 2$.

A. DUJELLA *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132**(2002), 23–33.

LEMMA 5 [Lemma 3, D.].
If $\{a, b, c\}$ is a Diophantine triple with the property $D(l)$ and $ab + l = r^2$, $ac + l = s^2$, $bc + l = t^2$, then there exist integers e, x, y, z such that

$$ae + l^2 = x^2, be + l^2 = y^2, ce + l^2 = z^2$$

and

$$c = a + b + \frac{e}{l} + \frac{2}{l^2}(abe + rxy).$$

Moreover, $e = l(a + b + c) + 2abc - 2rst$, $x = at - rs$, $y = bs - rt$, $z = cr - st$.

We use Lemma 5 for $l = -1$ and firstly proved the next result:

PROPOSITION 2
Let $m, n > 0$ and $b = n^2 + 1$. If $m|n$ and $t = m^2$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, b, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.

THEOREM 5.
Let $2p^k = q^{2^l} + 1, l > 0$, where p and q are odd primes.

(i) *If $t \in \{1, q^2, \ldots, q^{2^l-2}, q^{2^l}\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, 2p^k, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.*

(ii) *If $t \in \{q, q^3, \ldots, q^{2^l-3}, q^{2^l-1}\}$, then there does not exists a $D(-1)$-quadruple of the form $\{1, 2p^k, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$.*

$$x^2 - by^2 = \frac{1-b}{t} \qquad (9)$$

PROOF:
(i) Follows directly form Proposition 2.
(ii) Let us assume that $t \in \{q, q^3, \ldots, q^{2^l-3}, q^{2^l-1}\}$. In this case, the equation (9) is equivalent to

$$x^2 - (q^{2^l} + 1)y^2 = -q^s, \qquad (11)$$

where s is an odd integer and $0 < s \leq 2^l - 1$. Theorem 1 implies that the equation (11) has no integer solutions. Therefore, if $\{1, 2p^k, c, d\}$ is $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$, then $c, d > 0$. By the same argumentation as in Theorem 4 we conclude that such quadruple does not exist.

LEMMA 6 [Theorem 2.2, S.]

If $t > 0$, p is a prime and $\{1, p, c\}$ is a $D(-1)$-triple in the ring $\mathbb{Z}[\sqrt{-t}]$, then $c \in \mathbb{Z}$. Moreover, for every t there exists $c > 0$, while the case of $c < 0$ is possible if and only if $t|p-1$ and the equation

$$x^2 - py^2 = \frac{1-p}{t}$$

has an integer solution.

- the existence of $D(-1)$-quadruples of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}], t > 0$;
- the case of $p = 2$ is already proven;
- conjecture $p - 1 = q^{2j}, j \in \mathbb{N}$ leads us to the form $p = 2^{2^n} + 1, n \in \mathbb{N}$;
- considering Fermat prime greater then 3 (since 2 is not a square in $\mathbb{Z}[\sqrt{-t}]$).

So far, the only known such primes are $p = 5, 17, 257, 65537$, corresponding to $n = 1, 2, 3, 4$, respectively. The cases of $n = 1, 2$ which correspond to $p = 5, 17$ are solved in

I. SOLDO, *On the extensibility of $D(-1)$-triples $\{1, b, c\}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$*, Studia Sci. Math. Hungar., **50** (2013), 296–330.

The remaining cases are recently solved and presented in the paper

M. JUKIĆ BOKUN, I. SOLDO, *On the extensibility of $D(-1)$-pairs containing Fermat primes*, to appear in Acta Math. Hungar.

The results for so far known Fermat primes can be expressed in the form of the following theorem:

THEOREM 6.
Let $n \in \{1, 2, 3, 4\}$ and let p be the n-th Fermat prime. Let $t > 0$. If $t \in \{1, 2^2, \ldots, 2^{2^n-2}, 2^{2^n}\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$. In all other cases of t, in $\mathbb{Z}[\sqrt{-t}]$ does not exist $D(-1)$-quadruple of the previous form.

The proof of the above theorem is separated in few parts. The main steps are as follows:

In the research, whenever it was possible we proved some of our results on extendibility of a $D(-1)$-pair $\{1, p\}$ to a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}], t > 0$ for an arbitrary Fermat prime p. By using previous results we immediately have:

PROPOSITION 3
Let $n \geq 1$, p be the n-th Fermat prime, and let $t \in \{1, 2^2, \ldots, 2^{2^n-2}, 2^{2^n}\}$. There exist infinitely many $D(-1)$-quadruples of the form $\{1, p, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.

Suppose that there exists a $D(-1)$-quadruple of the form $\{1, p, c, d\}$, in $\mathbb{Z}[\sqrt{-t}], t > 0$.

For $t \nmid 2^{2^n} (= p - 1)$, we conclude that $c, d > 0$ and similarly obtain the contradiction with results in integers.

Keeping in mind the statement of Proposition 3, it remains to consider the cases of $t \in \{2, 2^3, \ldots, 2^{2^n-3}, 2^{2^n-1}\}$. They all satisfy the condition $t \mid 2^{2^n}$, so we have to consider weather the equations

$$x^2 - (2^{2^n} + 1)y^2 = -2^{2l+1}, \quad l \in \{0, 1, \ldots, 2^{n-1} - 1\}. \tag{12}$$

has an integer solution.

a) If $n = 1$ the only possibility is $l = 0$, i.e., $t = 2$ and the equation (12) has no solutions.
b) If $n \geq 2$, the solution does not exists for $l \in \{0, 1, \ldots, 2^{n-2} - 1\}$, i.e., in case of $t \in \{2^{2^{n-1}+1}, 2^{2^{n-1}+3}, \ldots, 2^{2^n-1}\}$.

PROPOSITION 4
Let $n \geq 1$ and let p be the n-th Fermat prime. There does not exist $D(-1)$-quadruple of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}], t > 0$ in the following cases:

a) $t \nmid 2^{2^n}$;

b) $n = 1$ and $t = 2$;

c) $n \geq 2$ and $t \in \{2^{2^{n-1}+1}, 2^{2^{n-1}+3}, \ldots, 2^{2^n-1}\}$.

It remains to consider the case of $n \geq 2$ and $l \in \{2^{n-2}, \ldots, 2^{n-1} - 1\}$, i.e., $t \in \{2, 2^3, \ldots, 2^{2^{n-1}-1}\}$. Here the integer solution of (12) exists and in that case at least one of c, d has to be negative integer (otherwise, we have the contradiction with extension in integers).

Since $\mathbb{Z}[\sqrt{-2^{2l+1}}] \subseteq \mathbb{Z}[\sqrt{-2}]$, it is enough to prove the nonexistence of such $D(-1)$-quadruple in the ring $\mathbb{Z}[\sqrt{-2}]$. Therefore, if $\tilde{s}, \tilde{t}, x, y, z \in \mathbb{Z}$, we will consider the existence of $D(-1)$-quadruples of the form $\{1, p, -c, -d\}$ and $\{1, p, -c, d\}$, where $c, d > 0$, corresponding to the following systems, respectively:

(i) $-c-1 = -2\tilde{s}^2$, $-pc-1 = -2\tilde{t}^2$, $-d-1 = -2x^2$, $-pd-1 = -2y^2$, $cd-1 = z^2$,

(ii) $-c-1 = -2\tilde{s}^2$, $-pc-1 = -2\tilde{t}^2$, $d-1 = x^2$, $pd-1 = y^2$, $-cd-1 = -2z^2$.

PROPOSITION 5

Let $n \geq 2$ and let p be the n-th Fermat prime. There does not exist a $D(-1)$-quadruple of the form $\{1, p, c, d\}$, $cd > 0$ in $\mathbb{Z}[\sqrt{-t}], t \in \{2, 2^3, \ldots, 2^{2^{n-1}-1}\}$.

PROPOSITION 6

Let $n = 3, 4$ and let p be the n-th Fermat prime. There does not exist a $D(-1)$-quadruple of the form $\{1, p, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}], t \in \{2, 2^3, \ldots, 2^{2^{n-1}-1}\}$.

Thank you for your attention!