On the sum of two divisors of $(n^2+1)/2$

Andrej Dujella and Florian Luca

1 Introduction

In [2], answering to a question from [1], Ayad and Luca proved that there does not exist an odd integer $n > 1$ and two positive divisors d_1 and d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = n + 1$. In this paper, we consider the similar problem but with $n+1$ replaced by an arbitrary linear polynomial $\delta n + \varepsilon$, where $\delta > 0$ and ε are given integers. Since the number $(n^2+1)/2$ is odd and both numbers d_1 and d_2 are congruent to 1 modulo 4, it follows that $d_1 + d_2 \equiv 2 \pmod 4$. Hence, if $d_1 + d_2 = \delta n + \varepsilon$, then either $\delta \equiv \varepsilon \equiv 1 \pmod 2$, or $\delta \equiv \varepsilon + 2 \equiv 0,\ 2 \pmod 4$. Here, we will restrict our attention to the first case, namely when both δ and ε are odd.

We will give some evidence for the following conjecture.

Conjecture 1 *If $\delta > 0$ and ε are coprime odd integers and $(\delta, \varepsilon) \neq (1,1)$, then there exist infinitely many positive odd integers n with the property that there exist a pair of positive divisors d_1 and d_2 of $(n^2+1)/2$ with $d_1 + d_2 = \delta n + \varepsilon$.*

We prove Conjecture 1 for $\delta = 1$. For general linear polynomials, we give a conditional proof relying on some known conjectures from the distribution of prime numbers. Both our unconditional and conditional proofs rely on known facts from the theory of Pell equations.

2 Monic polynomials – parametric solution

In this section, we look at polynomials of the form $n + \varepsilon$, where ε is an odd integer. We will show that the polynomial $n+1$ studied in [2] is the unique polynomial of this form for which there do not exist n, d_1 and d_2 with the property that we are considering.

Theorem 1 *For any odd integer $\varepsilon \neq 1$ there exist infinitely many odd positive integers n with the property that there exist a pair of positive divisors d_1 and d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = n + \varepsilon$.*

PROOF. Let ε be an odd integer. We want to find an odd positive integer n and positive divisors d_1 and d_2 of $(n^2+1)/2$ such that $d_1+d_2 = n+\varepsilon$. Let $g := \gcd(d_1, d_2)$ and write $d_1 = gd_1'$ and $d_2 = gd_2'$. Since $gd_1'd_2' = \mathrm{lcm}[d_1, d_2]$ divides $(n^2+1)/2$, we conclude that there exists a positive integer d such that

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

From the identity $(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1d_2$, we obtain easily that the equation

$$X^2 - d(d-2g)Y^2 = 2dg\varepsilon^2 + 2dg - 4g^2 \tag{1}$$

holds, where $X := (d-2g)n + \varepsilon d$ and $Y := d_2 - d_1$. Let us assume first that $g = 1$. Then equation (1) becomes

$$X^2 - d(d-2)Y^2 = 2d(\varepsilon^2+1) - 4. \tag{2}$$

The right hand side of equation (2) above is zero only when $2d(\varepsilon^2+1) = 4$, leading to $d = 1$, $\varepsilon = \pm 1$, and $X^2 + Y^2 = 0$. This is possible only when $X = Y = 0$, so, in particular, $d_1 = d_2$, which is not allowed. Thus, the right hand side in (2) is nonzero. Assuming further that $d > 2$, we get that (2) is a Pellian equation and therefore it will have infinitely many positive integer solutions (X, Y) provided that it has at least one such solution. To ensure that (2) has a solution, we take d such that the right hand side of (2) is a perfect square. This condition can be satisfied by taking

$$d = \frac{1}{2}(\varepsilon^2 - 4\varepsilon + 5).$$

With this choice for d, the well-known identity

$$z^4 + 1 = (z^2 - 2z + 2)(z^2 + 2z + 2),$$

yields easily that

$$2d(\varepsilon^2+1) - 4 = (\varepsilon - 1)^4.$$

Now we are left to search for the integer solutions (X, Y) of equation (2) of the form $X = (\varepsilon-1)^2 U$, $Y = (\varepsilon-1)^2 V^2$; i.e., such that

$$U^2 - d(d-2)V^2 = 1. \tag{3}$$

All the positive integer solutions (U, V) of equation (3) are given by $(U, V) = (U_m, V_m)$ for some $m \geq 0$, where

$$\begin{array}{c} U_0 = 1, \quad U_1 = d-1, \quad U_m = 2(d-1)U_{m-1} - U_{m-2}, \quad \text{for } m \geq 2, \\ V_0 = 0, \quad V_1 = 1, \quad V_m = 2(d-1)V_{m-1} - V_{m-2}, \quad \text{for } m \geq 2. \end{array} \tag{4}$$

It remains to compute the corresponding values of n arising from

$$(d-2)n + d\varepsilon = X = (\varepsilon - 1)^2 U^2 = (\varepsilon - 1)^2 {U_m}^2. \tag{5}$$

By induction on m using recurrence (4), one gets that $U_m \equiv 1 \pmod{(d-2)}$ for every $m \geq 0$. Thus,

$$(\varepsilon - 1)^2 {U_m}^2 - d\varepsilon \equiv (\varepsilon - 1)^2 - 2\varepsilon \equiv 2(d-2) \equiv 0 \pmod{(d-2)}.$$

Hence, the numbers n defined by (5) are integers, and since both d and ε are odd, the numbers n are also odd. The first few values of n with the corresponding divisors d_1 and d_2 of $(n^2+1)/2$ are listed below:

$$\begin{cases} n &= \varepsilon^2 - 3\varepsilon + 3, \\ d_1 &= 1, \\ d_2 &= \varepsilon^2 - 2\varepsilon + 2, \end{cases} \qquad \begin{cases} n &= \varepsilon^4 - 6\varepsilon^3 + 14\varepsilon^2 - 15\varepsilon + 7, \\ d_1 &= \varepsilon^2 - 2\varepsilon + 2, \\ d_2 &= \varepsilon^4 - 6\varepsilon^3 + 13\varepsilon^2 - 12\varepsilon + 5, \end{cases}$$

$$\begin{cases} n &= \varepsilon^6 - 10\varepsilon^5 + 41\varepsilon^4 - 88\varepsilon^3 + 104\varepsilon^2 - 65\varepsilon + 18 \\ d_1 &= \varepsilon^4 - 6\varepsilon^3 + 13\varepsilon^2 - 12\varepsilon + 5 \\ d_2 &= \varepsilon^6 - 10\varepsilon^5 + 40\varepsilon^4 - 82\varepsilon^3 + 91\varepsilon^2 - 52\varepsilon + 13. \end{cases}$$

Of course, as we already said, the above construction works only when $d > 2$, which is equivalent to $\varepsilon^2 - 5\varepsilon + 1 > 0$. This is true for all odd integers ε except when $\varepsilon \in \{1, 3\}$. Thus, we actually proved Theorem 1 for all $\varepsilon \notin \{1, 3\}$. The case $\varepsilon = 1$ is excluded, so let us deal now with $\varepsilon = 3$.

For the case $\varepsilon = 3$, we allow that $g \neq 1$. Certainly, g divides both $n + \varepsilon$ and $n^2 + 1$, so g divides $\varepsilon^2 + 1$. Thus, for $\varepsilon = 3$, the only possibility is $g = 5$. With these particular values, equation (1) becomes

$$X^2 - d(d-10)Y^2 = 100d - 100. \tag{6}$$

Equation (6) has solutions. For example, when $d = 101$, the fundamental solutions are $(X, Y) = (100, 0),\ (1920, \pm 20),\ (47168, \pm 492)$. For us, we need solutions with $X = 91n + 303$ and $n + 3 \equiv 0 \pmod 5$. The smallest such solution is $X = 1810020$. By periodicity, it is easy to see that there are

infinitely many such solutions. The first few values of n, with corresponding divisors d_1 and d_2 of $(n^2+1)/2$ are:

$$\begin{cases} n &= 19887, \\ d_1 &= 505, \\ d_2 &= 19385, \end{cases} \qquad \begin{cases} n &= 763267, \\ d_1 &= 19385, \\ d_2 &= 743885, \end{cases} \qquad \begin{cases} n &= 29289687, \\ d_1 &= 743885, \\ d_2 &= 28545805. \end{cases}$$

■

3 Polynomials with coprime coefficients – heuristic results

In this section, we consider general linear polynomials of the form $\delta n + \varepsilon$, where $\delta > 0$ and ε are coprime odd integers.

As in the previous section, we first transform our problem into a Pellian equation with an additional congruence condition on its solution. Define again the numbers g and d by

$$g := \gcd(d_1, d_2) \qquad \text{and} \qquad d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

Since g divides both $\delta n + \varepsilon$ and $(n^2+1)/2$, we find that g divides also $(\delta^2+\varepsilon^2)/2$. Furthermore, $g \equiv d \equiv 1 \pmod 4$. In this general case, the equation (1) takes the form

$$X^2 - d(d\delta^2 - 2g)Y^2 = 2dg(\delta^2+\varepsilon^2) - 4g^2, \tag{7}$$

where $X := n(d\delta^2 - 2g) + \delta\varepsilon d$.

Taking $g := (\delta^2+\varepsilon^2)/2$, the right hand side of equation (7) becomes $4g^2(d-1)$. We take $d = k^2+1$ with some even positive integer k and then the right hand side of equation (7) becomes the perfect square $(2gk)^2$. Now we have

$$d\delta^2 - 2g = (k^2+1)\delta^2 - (\delta^2+\varepsilon^2) = k^2\delta^2 - \varepsilon^2 = (\delta k + \varepsilon)(\delta k - \varepsilon),$$

and the equation (7) takes the form

$$X^2 - (k^2+1)(\delta k+\varepsilon)(\delta k-\varepsilon)Y^2 = (2gk)^2. \tag{8}$$

It is now clear that the equation (8) has infinitely many positive integer solutions (X, Y), but we need solutions which satisfy the additional condition

$$X \equiv \delta\varepsilon d \pmod{(\delta k+\varepsilon)(\delta k-\varepsilon)}. \tag{9}$$

Thus, we have to find even positive integers k for which there exists a solution of the Pell equation (8) that satisfies the condition (9). It is easy to see that if there exists one solution, then there will be infinitely many such solutions by the fact that binary recurrences related to solutions of Pell equations and norm form equations in real quadratic fields are totally periodic modulo any positive integer m.

To achieve the required goal, we take a positive integer k with the following properties:

(i) $\delta k + \varepsilon \equiv 5 \pmod 8$;

(ii) if $\varepsilon \equiv 1 \pmod 4$, then $\left(\frac{\delta^2+\varepsilon^2}{k^2+1}\right) = -1$;

(iii) if $\varepsilon \equiv 3 \pmod 4$, then $\left(\frac{\delta^2+\varepsilon^2}{\delta k-\varepsilon}\right) = -1$;

(iv) $\delta k + \varepsilon$ is a prime;

(v) $\delta k - \varepsilon$ is a prime;

(vi) $k^2 + 1$ is a prime.

First, let us see whether the above conditions can all be fulfilled simultenously. Observe that if (i) and (ii) are satisfied, then $4 \mid k$, therefore $k^2 + 1 \equiv 1 \pmod 8$. Since δ and ε are both odd, it follows that $\delta^2 + \varepsilon^2 \equiv 2 \pmod 8$, so $(\delta^2 + \varepsilon^2)/2$ is an odd integer which in fact is congruent to 1 (mod 4). Now by Quadratic Reciprocity, we have that in case (i) and (ii) hold, then

$$-1 = \left(\frac{\delta^2 + \varepsilon^2}{k^2 + 1}\right) = \left(\frac{2}{k^2 + 1}\right)\left(\frac{k^2 + 1}{(\delta^2 + \varepsilon^2)/2}\right) = \left(\frac{k^2 + 1}{(\delta^2 + \varepsilon^2)/2}\right).$$

We see that if $(\delta^2 + \varepsilon^2)/2$ is a perfect square, then the above equality is not possible. However, if $(\delta^2 + \varepsilon^2)/2$ is not a perfect square, then there exists k such that the above equality is possible. Indeed, clearly,

$$\left(\frac{k^2 + 1}{(\delta^2 + \varepsilon^2)/2}\right) = \prod_{i=1}^{s}\left(\frac{k^2 + 1}{p_i}\right),$$

where $p_1, \ldots, p_s$ are all the distinct primes appearing in the factorization of $(\delta^2 + \varepsilon^2)/2$ at odd exponents. Assume that $s \geq 1$. There exists a nonzero residue $x \pmod{p_1}$ such that $\left(\frac{x}{p_1}\right) = 1$ but $\left(\frac{x+1}{p_1}\right) = -1$. Indeed, otherwise

since $\left(\frac{1}{p_1}\right) = 1$, we would get that $\left(\frac{2}{p_1}\right) = 1$, next that $\left(\frac{3}{p_1}\right) = 1$, and so on. Thus, $\left(\frac{x}{p_1}\right) = 1$ for all $x = 1, \ldots, p_1 - 1$, which is a contradiction. So indeed there is a nonzero congruence class x modulo p_1 such that $\left(\frac{x}{p_1}\right) = 1$ and $\left(\frac{x+1}{p_1}\right) = -1$. Taking k such that $k^2 \equiv x \pmod{p_1}$ and $k \equiv 0 \pmod{p_i}$ for $i = 2, \ldots, s$, which is possible by the Chinese Remainder Lemma, we get that there is a residue class of k modulo $(\delta^2 + \varepsilon^2)/2$ such that condition (ii) holds.

An even easier argument shows that it is always possible to choose k modulo $(\delta^2 + \varepsilon^2)/2$ such that both conditions (i) and (iii) hold except when $(\delta^2 + \varepsilon^2)/2$ is a square. Indeed, by (i) and (iii), we get that $\delta k - \varepsilon \equiv 7 \pmod 8$, so

$$-1 = \left(\frac{\delta^2 + \varepsilon^2}{\delta k - \varepsilon}\right) = \left(\frac{2}{\delta k - \varepsilon}\right)\left(\frac{\delta k - \varepsilon}{(\delta^2 + \varepsilon^2)/2}\right) = \left(\frac{\delta k - \varepsilon}{(\delta^2 + \varepsilon^2)/2}\right),$$

and now a similar argument shows that indeed there is a value of k modulo $(\delta^2 + \varepsilon^2)/2$ such that both (i) and (iii) hold provided that $(\delta^2 + \varepsilon^2)/2$ is not a perfect square.

Next, let us recall a conjectural statement referred to as *Schinzel's Hypothesis H* (see [7]).

Conjecture 2 *Let $f_1(x), \ldots, f_s(x)$ be polynomials with integer coefficients and positive leading terms such as the following two conditions are satisfied:*

(i) $f_i(x)$ is irreducible for all $i = 1, \ldots, s$.

(ii) For each prime p there is a positive integer n such that

$$f_1(n) f_2(n) \cdots f_s(n) \not\equiv 0 \pmod{p}.$$

Then there exist infinitely many positive integers t such that

$$f_1(t),\ f_2(t),\ \ldots, f_s(t)$$

are simultaneously prime numbers.

From the above arguments and invoking again the Chinese Remainder Lemma, it follows assuming that $(\delta^2 + \varepsilon^2)/2$ is not a perfect square, that conditions (i) and (ii) (or (i) and (iii), respectively) are satisfied for all n in

a certain residue class a modulo $4(\delta^2+\varepsilon^2)$. Schinzel's Hypothesis H now applied to the three polynomials of t

$$\delta(4(\delta^2+\varepsilon^2)t+a)+\varepsilon, \qquad \delta(4(\delta^2+\varepsilon^2)t+a)-\varepsilon, \qquad (4(\delta^2+\varepsilon^2)t+a)^2+1$$

yields infinitely many values of t such that the numbers shown at (iv)–(vi) are simultaneously prime. Thus, all conditions (i)–(vi) should be fulfilled for infinitely many such positive integers k. In fact, an effective version of Schinzel's Hypothesis H due to Bateman and Horn [3] asserts that the number of such positive integers $k \le T$ should be

$$\gg \frac{T}{(\log T)^3},$$

for large values of T, where the implied constant depends on δ and ε.

With such values of k, consider now the Pell equation

$$U^2-(k^2+1)(\delta k-\varepsilon)(\delta k+\varepsilon)V^2=1. \tag{10}$$

We next show that the assumptions (i)–(vi) ensure that its fundamental solution in positive integers (U_0,V_0) satisfies

$$U_0 \equiv 1 \pmod{\delta k-\varepsilon}, \qquad \text{and} \qquad U_0 \equiv -1 \pmod{\delta k+\varepsilon}.$$

Indeed, with the notation $a:=k^2+1$, $b:=\delta k+\varepsilon$, $c:=\delta k-\varepsilon$, we have

$$U_0^2-1=abcV_0^2.$$

Since a, b and c are prime numbers, we have the following possibilities for the factors $U_0\pm 1$:

$1^{\pm})$ $U_0\pm 1=2abcs^2$, $U_0\mp 1=2t^2$;

$2^{\pm})$ $U_0\pm 1=2abs^2$, $U_0\mp 1=2ct^2$;

$3^{\pm})$ $U_0\pm 1=2acs^2$, $U_0\mp 1=2bt^2$;

$4^{\pm})$ $U_0\pm 1=2bcs^2$, $U_0\mp 1=2at^2$;

$5^{\pm})$ $U_0\pm 1=abcs^2$, $U_0\mp 1=t^2$;

$6^{\pm})$ $U_0\pm 1=abs^2$, $U_0\mp 1=ct^2$;

$7^{\pm})$ $U_0\pm 1=acs^2$, $U_0\mp 1=bt^2$;

$8^{\pm})$ $U_0 \pm 1 = bcs^2$, $U_0 \mp 1 = at^2$.

We want to show that only the cases $2^{+})$, $3^{-})$, $6^{+})$ and $7^{-})$ are possible.

The case $1^{+})$ implies $t^2 - abcs^2 = -1$, which is impossible since $bc = \delta^2 k^2 - \varepsilon^2 \equiv 3 \pmod 4$.

The case $1^{-})$ gives $t^2 - abcs^2 = 1$, which contradicts the minimality of (U_0, V_0).

In the case $2^{-})$, we have the equation $ct^2 - abs^2 = 1$, which is impossible modulo 4 since $a \equiv b \equiv 1 \pmod 4$ and $c \equiv 3 \pmod 4$, so that $ct^2 - abs^2 \not\equiv 1 \pmod 4$.

The equation in the case $3^{+})$ is $bt^2 - acs^2 = -1$, and this is again impossible modulo 4 since $b \equiv 1 \pmod 4$ and $ac \equiv 3 \pmod 4$.

The case $4^{+})$ leads to $at^2 - bcs^2 = -1$, which is impossible modulo 4.

In the case $4^{-})$, we have $at^2 - bcs^2 = 1$, which implies the conditions $(\frac{bc}{a}) = 1$ and $(\frac{a}{c}) = 1$. But

$$\left(\frac{bc}{a}\right) = \left(\frac{\delta^2 k^2 - \varepsilon^2}{k^2+1}\right) = \left(\frac{\delta^2(k^2+1) - (\delta^2+\varepsilon^2)}{k^2+1}\right) = \left(\frac{\delta^2+\varepsilon^2}{k^2+1}\right),$$

$$\left(\frac{a}{c}\right) = \left(\frac{(k^2+1)}{\delta k - \varepsilon}\right) = \left(\frac{(k^2+1)\delta^2 - (k^2\delta^2 - \varepsilon^2)}{\delta k - \varepsilon}\right) = \left(\frac{\delta^2+\varepsilon^2}{\delta k - \varepsilon}\right),$$

and the assumptions (ii) and (iii) show that both conditions above cannot be satisfied simultaneously.

The cases $5^{\pm})$ lead to $t^2 - abcs^2 = \mp 2$. Hence, $(\frac{\pm 2}{b}) = 1$, contradicting the assumption that $b \equiv 5 \pmod 8$.

The case $6^{-})$ leads to $ct^2 - abs^2 = 2$, which implies

$$\begin{aligned} 1 &= \left(\frac{-2ac}{b}\right) = -\left(\frac{2}{c}\right)\left(\frac{a}{c}\right)\left(\frac{b}{c}\right); \\ 1 &= \left(\frac{2c}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{c}{a}\right); \\ 1 &= \left(\frac{2c}{b}\right) = -\left(\frac{2}{b}\right). \end{aligned}$$

Multiplying the above three relations, we get $(\frac{2}{ac}) = 1$. But from $bc = \delta^2 k^2 - \varepsilon^2$, we conclude that if $k \equiv 0 \pmod 4$, then $a \equiv 1 \pmod 8$ and $c \equiv 3 \pmod 8$, while if $k \equiv 2 \pmod 4$, then $a \equiv 5 \pmod 8$ and $c \equiv 7 \pmod 4$. Hence, we always have $ac \equiv 3 \pmod 8$, so $(\frac{2}{ac}) = -1$, a contradiction.

The case 7^+) leads to $bt^2 - acs^2 = -2$, which implies

$$\begin{aligned} 1 &= \left(\frac{2ac}{b}\right) = -\left(\frac{a}{b}\right)\left(\frac{c}{b}\right); \\ 1 &= \left(\frac{-2b}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{b}{a}\right); \\ 1 &= \left(\frac{-2b}{c}\right) = -\left(\frac{2}{c}\right)\left(\frac{b}{c}\right). \end{aligned}$$

Multiplying the above three relations, we get $(\frac{2}{ac}) = 1$, contradicting the fact that $ac \equiv 3 \pmod 8$).

In the case 8^+); i.e., when $at^2 - bcs^2 = -2$, proceeding in a way similar to the previous two cases, we obtain the relation $(\frac{2}{ac}) = 1$, which leads to a contradiction.

In case 8^-); i.e., when $at^2 - bcs^2 = 2$, the relations become $(\frac{2}{a})(\frac{bc}{a}) = 1$, $(\frac{a}{b}) = -1$ and $(\frac{2}{c})(\frac{a}{c}) = 1$. If $\varepsilon \equiv 1 \pmod 4$, then $a \equiv 1 \pmod 8$, and the first relation is in contradiction with the assumption (ii). If $\varepsilon \equiv 3 \pmod 4$, the assumption (iii) gives $(\frac{a}{c}) = -1$, and since $c \equiv 7 \pmod 8$, we find that the third relation cannot hold.

Now take $X_0 := 2kgU_0$ and $Y_0 := 2kgV_0$. Then (X_0, Y_0) satisfies (7). Moreover,

$$\begin{aligned} X_0 &\equiv 0 \pmod g; \\ X_0 &\equiv 2kg \pmod{\delta k - \varepsilon}; \\ X_0 &\equiv -2kg \pmod{\delta k + \varepsilon}. \end{aligned}$$

We have to check that the number n defined by

$$X_0 := n(d\delta^2 - 2g) + \delta\varepsilon d$$

is an integer. Let

$$D := d\delta^2 - 2g = (\delta k - \varepsilon)(\delta k + \varepsilon).$$

We have

$$\delta X_0 \equiv 2kg\delta \equiv 2g\varepsilon \equiv d\delta^2\varepsilon \pmod{(\delta k - \varepsilon)}.$$

Since $\gcd(\delta, \varepsilon) = 1$, we obtain

$$X_0 \equiv \delta\varepsilon d \pmod{(\delta k - \varepsilon)}.$$

Similarly,

$$\delta X_0 \equiv -2kg\delta \equiv -2g \cdot (-\varepsilon) \equiv d\delta^2\varepsilon \pmod{(\delta k + \varepsilon)},$$

and we obtain

$$X_0 \equiv \delta\varepsilon d \pmod{(\delta k + \varepsilon)}.$$

Finally, we need that $\delta n + \varepsilon \equiv 0 \pmod{g}$. But $X_0 \equiv 0 \pmod{g}$ implies $nd\delta^2 + \delta\varepsilon d = (\delta n + \varepsilon)\delta d \pmod{g}$. Hence, $\delta n + \varepsilon \equiv 0 \pmod{g}$.

Thus, we obtained the following conditional result.

Proposition 1 *If Schinzel's Hypothesis H Conjecture 2 on prime values of polynomials is true, then for all coprime integers $\delta > 0$ and ε such that $2(\delta^2 + \varepsilon^2)$ is not a perfect square, there exist infinitely many odd positive integers n with the property that there exist a pair of positive divisors d_1 and d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = \delta n + \varepsilon$.*

Next, we give a particular example supporting Proposition 1.

Example 1 Let us consider the case $\delta = 3$ and $\varepsilon = 1$. There are 598 values of $k < 10^6$ which satisfy the properties (i)–(vi). The smallest such values are $4, 36, 116, 556, 644$.

Let us take $k = 4$. We then get $g = 5$ and $d = 17$. The fundamental solution of the equation (10) is $(U_0, V_0) = (189161350676, 3836541735)$. So, we obtain $X_0 = 2gkU = 7566454027040$, $Y_0 = 2kgV = 153461669400$, which gives the solution (n, d_1, d_2) with the desired property:

$$n = \frac{X_0 - 51}{143} = 52912265923, \;\; d_1 = 2637564185, \;\; d_2 = 156099233585.$$

4 The case when $2(\delta^2+\varepsilon^2)$ is a square - experimental results

The construction of the previous section cannot be applied to linear polynomials $\delta n + \varepsilon$ when $2(\delta^2 + \varepsilon^2)$ is perfect square. We have seen that in this case the properties (i)–(vi) cannot be simultaneously satisfied. However, the properties (iv)–(vi) are (conjecturally) satisfied by infinitely many values of k. This means that the fundamental solution (U_0, V_0) the equation (10), satisfies one of the systems $1^{\pm}$) – $8^{\pm}$); i.e, we have four possibilities for $U_0 \bmod \delta k \pm \varepsilon$:

$$U_0 \equiv \pm 1 \pmod{\delta k - \varepsilon}, \qquad U_0 \equiv \pm 1 \pmod{\delta k + \varepsilon}.$$

It seems plausible to assume that as the numbers k with properties (iv)–(vi) vary, the congruences $U_0 \equiv 1 \pmod{\delta k - \varepsilon}$, $U_0 \equiv -1 \pmod{\delta k + \varepsilon}$ hold with positive probability. Our experimental results support this assumption.

In particular, for all $\delta, |\varepsilon| < 100$, $|\delta\varepsilon| \neq 1$, $\gcd(\delta, \varepsilon) = 1$, we have found several numbers k with the desired property. For this purpose, we solved the corresponding Pell equations. When the larger values for k are needed, the solutions become too large to be found by the standard continued fraction algorithm. Instead, we used the compact representation algorithm recently implemented by F. Najman [6]. Here are some numerical data.

Example 2 For $(\delta, \varepsilon) = (7, 1)$, we have $k = 384$, and we obtain the fundamental solution $U_0 \approx 2.23797987 \cdot 10^{23417}$ which satisfies the required congruences and leads to a solution $n \approx 5.94701365 \cdot 10^{23414}$.

In the table below, we give the smallest k for each pair (δ, ε).

(δ, ε)	k	(δ, ε)	k
$(1, 7)$	54	$(1, -7)$	816
$(1, 41)$	1440	$(1, -41)$	150
$(7, 1)$	384	$(7, -1)$	1494
$(7, 23)$	210	$(7, -23)$	1080
$(7, 17)$	6480	$(7, -17)$	1350
$(17, 7)$	270	$(17, -7)$	1080
$(17, 31)$	306	$(17, -31)$	8424
$(17, 73)$	240	$(17, -73)$	5850
$(23, 7)$	270	$(23, -7)$	120
$(23, 47)$	11970	$(23, -47)$	25560
$(23, 89)$	4056	$(23, -89)$	150
$(31, 17)$	24	$(31, -17)$	126
$(31, 49)$	9120	$(31, -49)$	8670
$(41, 1)$	10560	$(41, -1)$	570
$(47, 23)$	54	$(47, -23)$	6360
$(47, 79)$	1290	$(47, -79)$	1320
$(49, 71)$	90	$(49, -71)$	240
$(71, 49)$	30720	$(71, -49)$	270
$(71, 97)$	240	$(71, -97)$	270
$(73, 17)$	10560	$(73, -17)$	2700
$(79, 47)$	66	$(79, -47)$	1176
$(89, 23)$	66	$(89, -23)$	11520
$(97, 71)$	54	$(97, -71)$	6360

5 Polynomials of the form $\delta n + \delta$

In this section, we consider a different generalization of the original problem from [2]. Namely, we replace the polynomial $n+1$ by the polynomial $\delta n+\delta$ for some positive integer δ.

Theorem 2 *Let δ be a positive integer. There does not exist an odd positive integer n with the property that there exist a pair of positive divisors d_1 and d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = \delta n + \delta$.*

Proof. By the main result from [2], we know that the statement is true for $\delta = 1$. From the relation $d_1 + d_2 = \delta(n+1)$, as well as the fact that $d_1 \equiv$

$d_2 \equiv 1 \pmod 4$, we conclude that δ is odd. Let δ be the smallest positive integer for which the statement is not true, and let the triple (n, d_1, d_2) satisfy the property from the theorem. Put $g := \gcd(d_1, d_2)$. Then $g \mid \delta^2$. Assume that $g > 1$. Then there exists a prime p dividing both g and δ. Let $d_1 = pd_1'$, $d_2 = pd_2$, $\delta = p\delta'$. Then d_1' and d_2' are divisors of $(n^2+1)/2$ and $d_1' + d_2' = \delta' n + \delta'$, contradicting the minimality of δ.

Thus, $g = 1$ and the equation (7) takes the form

$$X^2 - (d^2\delta^2 - 2d)Y^2 = 4(d\delta^2 - 1). \tag{11}$$

We need a positive integer solution X of the above equation satisfying the congruence

$$X \equiv d\delta^2 \equiv 2 \pmod{d\delta^2 - 2}. \tag{12}$$

From $d_1 d_2 = (n^2+1)/(2d)$, we find that $d \equiv 1 \pmod 4$. Hence, $d^2\delta^2 - 2d \equiv 7 \pmod 8$, and this implies that $X \equiv Y \equiv 0 \pmod 4$. Let $X = 4S$, $Y = 4T$, so that

$$S^2 - (d^2\delta^2 - 2d)T^2 = \frac{d\delta^2 - 1}{4}. \tag{13}$$

Let $u := \gcd(S, T)$, $S := uU$, $T := uV$. From (13), we find that

$$\left| \sqrt{d^2\delta^2 - 2d} - \frac{U}{V} \right| < \frac{(d\delta^2 - 1)/(4u^2)}{2\sqrt{d^2\delta^2 - 2d}} V^{-2} < \frac{\delta + 1}{8u^2} V^{-2}.$$

From Worley's theorem from Diophantine approximations (see [8, Theorem 1] and [4, Theorem 1]), we conclude that there exist nonnegative integers k, r, s, $rs < (\delta+1)/(4u^2)$, such that

$$U = rp_k \pm sp_{k-1}, \qquad \text{and} \qquad V = rq_k \pm sq_{k-1},$$

where p_k/q_k denotes the kth convergent in the continued fraction expansion of $\sqrt{d^2\delta^2 - 2d}$. Since $\delta \geq 3$, the continued fraction expansion of $\sqrt{d^2\delta^2 - 2d}$ is

$$[d\delta - 1; \overline{1, \delta - 2, 1, 2d\delta - 2}].$$

By [5, Lemma 1], we have

$$\begin{aligned}(rp_k + sp_{k-1})^2 - (d^2\delta^2 - 2d)(rq_k + sq_{k-1})^2 = \\ (-1)^k(s^2\tau_k + 2rs\sigma_{k+1} - r^2\tau_{k+1}),\end{aligned} \tag{14}$$

where

$$\begin{aligned}
(\sigma_0, \tau_0) &= (0, 1), \\
(\sigma_1, \tau_1) &= (d\delta - 1, 2d\delta - 2d - 1), \\
(\sigma_2, \tau_2) &= (2\delta - 2d, 2d), \\
(\sigma_3, \tau_3) &= (d\delta - 2d, 2d\delta - 2d - 1), \\
(\sigma_4, \tau_4) &= (d\delta - 1, 1), \\
(\sigma_{k+4}, \tau_{k+4}) &= (\sigma_k, \tau_k) \qquad \text{for all} \qquad k \geq 1.
\end{aligned}$$

The sequence $\{p_k\}_{k\geq 0}$ modulo $d\delta^2 - 2$ is periodic with the period length 4. Indeed,

$$p_0 = d\delta - 1, \quad p_1 = d\delta, \quad p_2 \equiv -d\delta + 1 \bmod d\delta^2 - 2, \quad p_3 \equiv 1 \bmod d\delta^2 - 2,$$

and

$$p_k \equiv p_{k-4} \pmod{d\delta^2 - 2} \qquad \text{for} \qquad k \geq 4.$$

Hence, we have

$$rp_k + sp_{k-1} \in \{d\delta(r \pm s) \mp s,\ d\delta(-r \pm s) + r,\ \mp d\delta s + r,\ d\delta r + (-r \pm s)\}$$

modulo $d\delta^2 - 2$.

Assume first that $u > \sqrt{(\delta - 1)/2}$. Then $rs \leq (\delta - 1)/(4u^2) < 1$, and thus $U = p_k$, $V = q_k$. By (14), we have

$$p_k^2 - (d^2\delta^2 - 2d)q_k^2 = (-1)^{k+1}t_{k+1} \in \{1, -2d\delta + 2d + 1, 2d\}.$$

It is clear that $(d\delta^2 - 1)/(4u^2) \neq -2d\delta + 2d + 1$ since these numbers have different signs. Also, the equality $(d\delta^2 - 1)/(4u^2) = 2d$ is not possible unless $d = 1$. So let us consider the equation

$$U^2 - (d^2\delta^2 - 2d)V^2 = 1.$$

The sequence of its positive integer solutions $\{U_m\}_{m\geq 0}$ starts as

$$1,\ d\delta^2 - 1,\ 2(d\delta^2 - 1)^2 - 1,\ \ldots.$$

From here, we see easily that $U \equiv 1 \pmod{d\delta^2 - 2}$. Hence, $X \equiv 4u \pmod{d\delta^2 - 2}$. But, by (12), we should have also $X \equiv 2 \pmod{d\delta^2 - 2}$. Hence, $d\delta^2 - 2$ divides $4u - 2$. However, this implies that $4u^2 - 1 = d\delta^2 - 2 \leq 4u - 2$, a contradiction.

Assume now that $u \leq \sqrt{(\delta-1)/2}$. We have $X = 4uU \equiv 4u(d\delta A + B) \pmod{d\delta^2 - 2}$, where $|A|, |B| \leq r + s$. We have $r + s \leq (\delta - 1)/(4u^2) + 1$, and thus,

$$4u(d\delta A + B) \leq \frac{16}{3} ud\delta \left(\frac{\delta - 1}{4u^2} + 1 \right) \leq \frac{16}{3} d\delta \left(\frac{\delta - 1}{4u} + u \right).$$

On the other hand, by (12), $4u(d\delta A + B) = 2 + C(d\delta^2 - 2)$, for some even integer C. If δ is large enough, say $\delta > 7$, then $4u(d\delta A + B) < 2 + 2(d\delta^2 - 2)$, and therefore we must have $4u(d\delta A + B) = 2$, which is a contradiction.

Therefore, it only remains to consider small values for d and δ. For $\delta = 3, 5, 7$, we have $u \leq \sqrt{(\delta - 1)/2} < 2$; i.e., $u = 1$. Also, $rs \leq (\delta - 1)/4 < 1$; i.e., $U = p_k$ and $V = q_k$, and we obtain a contradiction as before.

Finally, let $d = 1$. It remains to consider the possibility that $(\delta^2 - 1)/(4u^2) = 2$; i.e., $\delta^2 - 1 = 8u^2$. Now the equation (13) becomes

$$U^2 - (\delta^2 - 2)V^2 = 2. \tag{15}$$

The sequence of positive integer solutions $\{U_m\}_{m \geq 1}$ of (15) starts as

$$\delta,\ 2\delta^3 - 4\delta,\ 4\delta^5 - 10\delta^3 + 5\delta, \ldots.$$

Hence, we have $U \equiv \delta \pmod{\delta^2 - 2}$. But we should also have $X = 4uU \equiv 2 \pmod{\delta^2 - 2}$. Thus, $\delta^2 - 2$ divides $4u\delta - 2$, which implies $(\delta^2 - 2)z = 4u\delta - 2$ for an even integer z. However,

$$4u\delta - 2 < 4\delta \cdot \frac{\delta}{\sqrt{8}} - 2 = \sqrt{2}\delta^2 - 2 < 2(\delta^2 - 2),$$

a contradiction. ∎

Acknowledgements: We thank the referee for a careful reading of the paper and for several constructive comments on an earlier version of the manuscript. This work started during a very pleasant visit of F. L. at the Mathematics Department of the University of Zagreb in February of 2009. This author thanks the people of that Department for their hospitality. A. D. was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821, and F. L. was also supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] M. Ayad, *Critical points, critical values of a prime polynomial*, Complex Var. Elliptic Equ. **51** (2006), 143–160.

[2] M. Ayad and F. Luca, *Two divisiors of* $(n^2+1)/2$ *summing up to* $n+1$, J. Théor. Nombres Bordeaux **19** (2007), 561–566.

[3] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363—367.

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

[5] A. Dujella and B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

[6] F. Najman, *Compact representation of quadratic integers and integer points on some elliptic curves*, Rocky Mountain J. Math., to appear.

[7] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208, Corrigendum, **5** (1959), 259.

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

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb
Croatia
E-mail: duje@math.hr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán
México
E-mail: fluca@matmor.unam.mx