Journal de Théorie des Nombres
de Bordeaux **19** (2007), 561–566

Two divisors of $(n^2+1)/2$ summing up to $n+1$

par Mohamed AYAD et Florian LUCA

Résumé. Dans cette courte note, on donne une réponse affirmative à une question d'Ayad posée dans [1].

Abstract. In this short note, we give an affirmative answer to a question of Ayad from [1].

1. Main result

In [1], Mohamed Ayad asked to prove that there does not exist an odd prime p and two positive divisors d_1 and d_2 of $(p^2+1)/2$ such that $d_1+d_2 = p+1$. In this note, we prove a bit more, namely:

Theorem 1.1. *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 $d_1+d_2 = n+1$.*

The condition $n>1$ cannot be dropped since for $n=1$ we may take $d_1 = d_2 = 1$.

Proof. Let $n>1$ be an odd integer for which there exist two divisors d_1 and d_2 as in the statement of the theorem. Since n is odd, we get that $n^2 \equiv 1 \pmod 8$, therefore $(n^2+1)/2$ is odd. We show that d_1 and d_2 are coprime. Indeed, if not there exists an odd prime $q \mid \gcd(d_1, d_2)$. Hence, $q \mid d_1+d_2$, therefore $n \equiv -1 \pmod q$. Since also $q \mid d_1 \mid n^2+1$, we get that $n^2 \equiv -1 \pmod q$. From the above two congruences we obtain that $(-1)^2 \equiv -1 \pmod q$, so $q \mid 2$, which is impossible.

Since d_1 and d_2 divide $(n^2+1)/2$ and are coprime, we get that $d_1 d_2 \mid (n^2+1)/2$. Write $d_1 d_2 = (n^2+1)/(2d)$. Then

$$(d_1-d_2)^2 = (d_1+d_2)^2 - 4d_1d_2 = (n+1)^2 - 2\left(\frac{n^2+1}{d}\right)$$
$$= \frac{((d-2)n+d)^2 + 4 - 4d}{d(d-2)}.$$

Now notice that all divisors of n^2+1 are congruent to 1 modulo 4. In particular, this applies to d_1, d_2 and d. Hence, $n = d_1+d_2-1$ is congruent

Manuscrit reçu le 26 septembre 2006.

to 1 modulo 4 as well. It follows that

$$X = \left|\frac{(d-2)n+d}{4}\right|, \qquad Y = \left|\frac{d_1-d_2}{4}\right|, \qquad s = \frac{d-1}{4}$$

are non-negative integers satisfying

$$X^2 - DY^2 = s, \tag{1.1}$$

with $D = d(d-2) = (4s)^2 - 1$. If $s = 0$, then $X^2 + Y^2 = 0$, so $Y = 0$, leading to $d_1 = d_2$. Since these two divisors are also coprime, we get that $d_1 = d_2 = 1$, therefore $n + 1 = d_1 + d_2 = 2$, contradicting the fact that $n > 1$. Hence, we may assume that $s \geq 1$. The above Diophantine equation (1.1) leads to

$$\left|\frac{X}{Y} - \sqrt{D}\right| = \frac{s}{Y(X + \sqrt{D}Y)}.$$

Note that $X > Y\sqrt{D}$, therefore $X + \sqrt{D}Y > 2\sqrt{D}Y > 2sY$, because $\sqrt{D} = \sqrt{(4s)^2 - 1} > s$, therefore

$$\left|\frac{X}{Y} - \sqrt{D}\right| < \frac{1}{2Y^2}.$$

It is a known criterion due to Legendre that the above inequality implies that X/Y must be a convergent of $\sqrt{D}$. With $\lambda = 4s$, it is easily checked that we have the following continued fraction expansion

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

where $\{\ldots\}$ emphasizes the period. Using the above continued fraction, one checks easily that if p_m/q_m denotes the mth convergent to $\sqrt{\lambda^2 - 1}$, then $p_m^2 - Dq_m^2 = -2\lambda + 2$ or 1, according to whether m is even or odd. Hence, for our values of X and Y we should have that

$$X^2 - DY^2 \in \{-8s + 2, 1\},$$

and comparing it with equation (1.1) we get that the only chance is $s = 1$, leading to $d = 5$ and $D = 15$. Hence, (X, Y) is a solution of the Pell equation

$$X^2 - 15Y^2 = 1. \tag{1.2}$$

The minimal solution of the above Pell equation is $(X_1, Y_1) = (4, 1)$. Hence, if we write (X_t, Y_t) for the tth solution of Pell equation (1.2), we then get that

$$X_t + \sqrt{15}Y_t = (4 + \sqrt{15})^t \qquad \text{holds for all } t \geq 1.$$

Using the above representation, one checks easily that $X_t \equiv 1 \pmod 3$ for all positive integers t. Thus, if $X_t = s(n+1) - (n-1)/4 = (n+1) - (n-1)/4$ for some positive integer n, we would then get that $n = (4X_t - 5)/3$, but since $4X_t - 5 \equiv -1 \pmod 3$, we get that $(4X_t - 5)/3$ is never an integer

for any positive integer t. Thus, there is no solution and the theorem is completely proved. □

2. Applications

Next, we present a corollary to Theorem 1.1 which has already been proved in [1] by a different method.

Corollary 2.1. *Let p be an odd prime number. Let a and b be two distinct complex numbers. Then any primitive of the polynomial*

$$((x-a)(x-b))^{(p^2-1)/2}$$

is indecomposable over $\mathbb{C}$.

Proof. In order to prove the above corollary we will need, aside from Theorem 1.1, to recall a result from [1]. Let $f(x)$ be a polynomial with complex coefficients of degree m. Let F be the set of the critical points of $f(x)$ and assume that F contains r elements. For any $z \in F$ denote by $\nu_f(z)$ the valency of z; i.e., $\nu_f(z) = m_{f'}(z) + 1$, where $m_{f'}(z)$ is the multiplicity of z as a root of f'. Assume that $f = g \circ h$, where g and h are polynomials with complex coefficients of degree at least 2. Let $k = \deg h$. It is then proved in [1] that there exist distinct elements $x_1, \dots, x_s$ in F, and positive divisors $d_1, \dots, d_s$ of $\nu_f(x_1), \dots, \nu_f(x_s)$, respectively, such that $1 < d_i \le \nu_f(x_i)$ and $k - 1 = \sum_{i=1}^{i=s}(d_i - 1)$.

We can now embark to the proof of Corollary 2.1. Let $f(x)$ be a primitive of $((x-a)(x-b))^{(p^2-1)/2}$. Suppose that there exits some non-trivial decomposition of $f(x)$ in the form $f(x) = g(h(x))$. Since $\deg f = p^2$, we get that $k = \deg h = p$. With the previous notations, we have $F = \{a, b\}$, and $\nu_f(a) = \nu_f(b) = (p^2+1)/2$. If $s = 1$, then $k = p$ divides $(p^2+1)/2$, which is clearly impossible. Thus, $s = 2$ and there exist two positive divisors d_1 and d_2 of $(p^2+1)/2$ such that $k-1 = p-1 = d_1 - 1 + d_2 - 1$. However, this is impossible by Theorem 1, which completes the proof of Corollary 1. □

Finally, we present a Diophantine application of Corollary 2.1. Let $a < b$ and $c < d$ be integers, e be an integer and p and q be odd primes. Consider the Diophantine equation

$$\int_0^x ((t-a)(t-b))^{(p^2-1)/2}\,dt - \int_0^y ((s-c)(s-d))^{(q^2-1)/2}\,ds = e \tag{2.1}$$

in integer solutions (x, y). In some cases, it can have infinitely many integer solutions (x, y). Indeed, suppose that $p = q$ and that $c - a = d - b = f$.

Then,

$$\begin{aligned}\int_0^y ((s-c)(s-d))^{(q^2-1)/2}\,ds &= \int_0^y ((s-a-f)(s-b-f))^{(p^2-1)/2}\,ds\\ &= \int_{-f}^{y-f} ((t-a)(t-b))^{(p^2-1)/2}\,dt\\ &= \int_0^{y-f} ((t-a)(t-b))^{(p^2-1)/2}\,dt + h,\end{aligned}$$

where $h = \int_{-f}^{0} ((t-a)(t-b))^{(p^2-1)/2}\,dt$, so equation (2.1) is

$$F(x) - F(y-f) = e_1,$$

where $F(x) = \int_0^x ((t-a)(t-b))^{(p^2-1)/2}\,dt$ and $e_1 = e + h = e - F(-f)$. If $e_1 = 0$, then the above equation has infinitely many solutions (namely $x = y - f$).

The next corollary shows that the above instance is the only one in which the Diophantine equation (2.1) can have infinitely many integer solutions (x, y).

Corollary 2.2. *Let $a < b$, $c < d$, $p \le q$ and e be fixed integers, where p and q are odd primes. If the Diophantine equation* (2.1) *has infinitely many integer solutions x, y, then $p = q$, $c - a = d - b = f$ and $e = \int_0^{-f} ((t-a)(t-b))^{(p^2-1)/2}\,dt$.*

Proof. Assume that $p \le q$ and that the given equation has infinitely many positive integer solutions x, y. Let $F(x) = \int_0^x ((t-a)(t-b))^{(p^2-1)/2}\,dt$ and $G(x) = \int_0^x ((t-c)(t-d))^{(q^2-1)/2}\,dt + e$. By Corollary 2.1, both $F(x)$ and $G(x)$ are indecomposable. By the main finiteness criterion from [3], it follows that $(F(x), G(x)) = (\phi \circ u \circ \kappa(x), \phi \circ v \circ \ell(x))$, where $\phi(x) \in \mathbb{Q}[X]$ is a non-constant polynomial, $\kappa(x)$ and $\ell(x)$ are linear polynomials in $\mathbb{Q}[x]$ and the pair of polynomials $(u(x), v(x))$ belongs to five kinds of standard pairs, which are all listed both in [3] as well as on page 182 of [2]. Since for us F and G are indecomposable, it follows that either ϕ is linear or both u and v are linear polynomials.

Assume first that ϕ is linear. Note that for us the critical sets of $F(x)$ and $G(x)$ are $\mathcal{F} = \{a, b\}$ and $\mathcal{G} = \{c, d\}$ respectively. Furthermore, the two critical points in $\mathcal{F}$ have the same valency and the same is true for $\mathcal{G}$. In what follows, α and β are non-zero rational numbers, μ, ν, d are positive integers, ρ is a non-negative integer and $\nu(x) \in \mathbb{Q}[X]$ is a non-zero polynomial which may be constant.

Since the *standard pair of the first kind* is $(x^d, \alpha x^\rho \nu(x)^d)$, where $0 \le \rho < d$, $\gcd(\rho, d) = 1$, $\rho + \deg \nu(x) > 0$ (or switched), it follows that in such pairs

one of the polynomials has a critical set consisting of at most one element. Hence, $(F(x), G(x))$ cannot be equal to $(\phi \circ u \circ \kappa(x), \phi \circ v \circ \ell(x))$ for some linear polynomials $\phi(x)$, $\kappa(x)$ and $\ell(x)$ and a standard pair of the first kind $(u(x), v(x))$.

Since *the standard pair of the second kind* is $(x^2, (\alpha x^2+\beta)\nu(x)^2)$ (or switched), it follows as in the previous case that in such pairs one of the polynomials has a critical set consisting of at most one element, and the same contradiction as in the previous case is obtained.

To introduce standard pairs of third and fourth kind, we need to introduce the Dickson polynomials. Denote by $D_\mu(x,\delta)$ the μth Dickson polynomial defined by the functional equation

$$D_\mu(z+\delta/z, \delta) = z^\mu + (\delta/z)^\mu,$$

or explicitly by

$$D_\mu(z,\delta) = \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} z^{\mu-2i}, \qquad \text{where} \qquad d_{\mu,i} = \frac{\mu}{\mu-i}\binom{\mu-i}{i}(-\delta)^i.$$

Then the *standard pairs of third and fourth kind* are the pairs of the form $(D_\mu(x,\alpha^\nu), D_\nu(x,\alpha^\mu))$, where $\gcd(\mu,\nu)=1$, together with the pairs $(\alpha^{-\mu/2}D_\mu(x,\alpha), -\beta^{-\nu/2}D_\nu(x,\beta))$, where $\gcd(\mu,\nu)=2$, respectively. It is known that the derivatives of the Dickson polynomials have only simple roots (a verification of this simple fact is done at the end of Section 6 in [4], for example). Since for us all roots of both F' and G' are of multiplicity larger than 1, we get that $(F(x), G(x))$ cannot be equal to $(\phi \circ u \circ \kappa(x), \phi \circ v \circ \ell(x))$ for some linear polynomials $\phi(x)$, $\kappa(x)$ and $\ell(x)$ and a standard pair of the third or fourth kind $(u(x), v(x))$.

Finally, *a standard pair of the fifth kind* is $((\alpha x^2-1)^2, 3x^4-4x^3)$ (or switched) which have degrees at most 4, whereas $\deg g = (q^2+1)/2 \geq (3^2+1)/2 \geq 5$, so again $(F(x), G(x))$ cannot be equal to $(\phi \circ u \circ \kappa(x), \phi \circ v \circ \ell(x))$ for some linear polynomials $\phi(x)$, $\kappa(x)$ and $\ell(x)$ and a standard pair of the fifth kind $(u(x), v(x))$.

Assume now that ϕ is not linear. Then $\deg F = \deg G$, therefore $p=q$. Further, we may take $u(x)=v(x)=x$. Let $\kappa(x)=\kappa_1 x+\kappa_0$ and $\ell(x)=\ell_1 x+\ell_0$. Identifying the leading coefficients in $F(x)=\phi(u((\kappa(x)))$ and $G(x)=\phi(v(\ell(x)))$, respectively, we get that $a_0\kappa_1^{(p^2+1)/2} = a_0\ell_1^{(p^2+1)/2} = 2/(p^2+1)$, where $a_0 \neq 0$ is the leading coefficient of $\phi(x)$. Hence, $\kappa_1^{(p^2+1)/2} = \ell_1^{(p^2+1)/2}$ and since $(p^2+1)/2$ is odd, we get that $\kappa_1 = \ell_1$. Thus,

$$G(x) = \phi(\kappa_1 x + \ell_0) = \phi(\kappa_1(x + (\ell_0-\kappa_0)/\kappa_1) + \kappa_0) = F(x-f),$$

where $f = -(\ell_0 - \kappa_0)/\kappa_1$. Taking derivatives we get $G'(x) = F'(x - f)$, so

$$((x-c)(x-d))^{(p^2-1)/2} = ((x-f-a)(x-f-b))^{(p^2-1)/2};$$

hence, $c - a = d - b = f$. The statement about e is now immediate. □

Acknowledgements. We thank the referee for useful suggestions and for a simplification of our original proof of Theorem 1.1. This work was done in May of 2006, while both authors attended the conference on *Congrès International, Algèbre, Théorie des Nombres et leurs Applications* at the University Mohammed I, in Oujda, Morocco. They thank the organizers for the opportunity of participating in this event. During the preparation of this paper, F. L. was also supported in part by grants PAPIIT IN104505, SEP-CONACyT 46755 and a Guggenheim Fellowship.

References

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

[2] Yu. F. Bilu, B. Brindza, P. Kirschenhofer, A. Pintér and R. F. Tichy, *Diophantine equations and Bernoulli polynomials. With an appendix by A. Schinzel*. Compositio Math. **131** (2002), 173–188.

[3] Yu. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*. Acta Arith. **95** (2000), 261–288.

[4] Y. Bugeaud and F. Luca, *On Pillai's Diophantine equation*. New York J. Math. **12** (2006), 193–217.

Mohamed Ayad
Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral
F-62228 Calais, France
E-mail : ayad@lmpa.univ-littoral.fr

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