QUADRATIC FORMS REPRESENTING pTH TERMS OF LUCAS SEQUENCES

PEDRO BERRIZBEITIA, ROBIN CHAPMAN, FLORIAN LUCA, AND ALBERTO MENDOZA

ABSTRACT. We prove that if $\{A_n\}_{n\geq 0}$ is any Lucas sequence and p is any prime, then $4A_p$ admits a representation by one of two quadratic forms according to the residue class of p modulo 4.

1. Introduction

Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. The starting point for the investigation of the subject in the title is the formula

$$F_{2n+1} = F_n^2 + F_{n+1}^2 \tag{1}$$

known to Lucas (take $Q = -1$ in formula (34) in Lucas's seminal 1878 paper [4]) since it implies that every Fibonacci number of odd index can be represented as the sum of two squares of integers. This is a question which leads naturally to the investigation of Fibonacci numbers F_n which can be represented under the form $au^2 + buv + cv^2$ with some integers u and v and some integers a, b and c which can be either fixed or depend on n. For example, in [6], it is shown that if $n \equiv 7 \pmod{16}$, then $F_n = u^2 + 9v^2$ holds with some positive integers u and v. For general results regarding the problem of the kind $F_n = u^2 + dv^2$, when d is fixed, see [3].

In [2], it was noted that if $n = p^2$ is the square of an odd prime $p \neq 5$, then p divides $F_{\frac{p^2-1}{2}}$, hence formula (1) implies that $F_{p^2} = u^2 + p^2v^2$, for some integers u and v. Motivated by this observation, the authors of [2] introduced and estimated the counting function of the infinite set

$$S = \{n \ : \ F_n = u^2 + nv^2 \text{ with some integers } u, v\}.$$

In the course of their investigation, they found computational evidence that indicated that every prime $p \equiv 1 \pmod 4$ belongs to S. In [1], it was proved that this fact is true; that is if $p \equiv 1 \pmod 4$, then $F_p = u^2 + pv^2$ for some integers u and v. The proof makes use of basic facts in Galois Theory and basic properties of the norm function of finite extensions of $\mathbb{Q}$. Prior, it was shown in [6] that the above formula never holds if instead of $p \equiv 1 \pmod 4$, we have $p \equiv 3, 7$

Date: 10th November 2016.

(mod 20). In this paper, we extend the results of [1] from the Fibonacci sequence to any Lucas sequence of integers. That is, using basic Galois theory, we find representations by quadratic forms of $4A_p$ for all primes p (congruent to either 1 or 3 modulo 4), where $\{A_n\}_{n\geq 0}$ is any Lucas sequence of integers.

2. The result

Fix integers r and s and consider the Lucas sequence given by

$$A_0 = 0, \quad A_1 = 1, \qquad A_n = rA_{n-1} + sA_{n-2} \quad \text{for all} \quad n \geq 0.$$

We exclude the case in which the roots (α, β) of the quadratic equation $x^2 - rx - s = 0$ are equal. The case $r = s = 1$ gives $A_n = F_n$. Define the *discriminant* of this sequence as $D = r^2 + 4s$. Note that $D \neq 0$ because $\alpha \neq \beta$.

Theorem 1.

(1) *If $p \equiv 1 \pmod 4$ is prime, then A_p is represented by the quadratic form $u^2 + uv - \frac{1}{4}(p-1)v^2$ and $4A_p$ is represented by the quadratic form $u^2 - pv^2$.*

(2) *If $p \equiv 3 \pmod 4$ is prime, then $4A_p$ is represented by the quadratic form $Du^2 + pv^2$.*

3. The proof

The sequence A_n is given explicitly by

$$A_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for all} \qquad n \geq 0.$$

We take

$$\alpha = \frac{r + \sqrt{D}}{2}, \qquad \beta = \frac{r - \sqrt{D}}{2}.$$

Note that $\alpha + \beta = r$, $\alpha\beta = -s$ and $\alpha - \beta = \sqrt{D}$.

For a positive integer n let ζ_n be a primitive nth root of unity.

For an odd prime p,

$$A_p = \prod_{j=1}^{p-1} (\alpha - \zeta_p^j \beta) = F(\alpha, \beta) G(\alpha, \beta),$$

where we define

$$F(x, y) = \prod_{j \in R} (x - \zeta_p^j y), \qquad G(x, y) = \prod_{j \in N} (x - \zeta_p^j y),$$

where R and N are, respectively, the sets of quadratic residues and quadratic nonresidues modulo p. Then

$$F(y, x) = \prod_{j \in R} (y - \zeta_p^j x) = (-1)^{(p-1)/2} \zeta_p^S \prod_{j \in R} (x - \zeta_p^{-j} y),$$

where

$$S = \sum_{j \in R} j.$$

Now

$$S \equiv \sum_{k=1}^{(p-1)/2} k^2 \equiv p\left(\frac{p^2-1}{24}\right) \pmod{p}.$$

As long as $p \geq 5$, 24 divides (p^2-1), so $p \mid S$, therefore $\zeta_p^S = 1$. We will return to the case $p = 3$ at the end, so let us continue assuming that $p \geq 5$.

If $p \equiv 1 \pmod 4$, then $(-1)^{(p-1)/2} = 1$ and $-1 \in R$ so that $F(y,x) = F(x,y)$ in this case. A similar argument gives $G(y,x) = G(x,y)$.

If $p \equiv 3 \pmod 4$, then $(-1)^{(p-1)/2} = -1$ and $-1 \in N$ so that $F(y,x) = -G(x,y)$ and consequently $G(y,x) = -F(x,y)$.

The polynomial $F(x,y)$ has coefficients which are algebraic integers in $\mathbf{Q}(\zeta_p)$ and which are fixed under all automorphisms of the form σ_j (where $\sigma_j : \zeta_p \mapsto \zeta_p^j$) for $j \in R$. Thus these coefficients lie in the quadratic subfield of $\mathbf{Q}(\zeta_p)$, which is $\mathbf{Q}(\sqrt{p^*})$, with $p^* = (-1)^{(p-1)/2}p$. The ring of integers of $\mathbf{Q}(\sqrt{p^*})$ is $\mathbf{Z}[(1+\sqrt{p^*})/2]$, and so

$$F(x,y) = F_1(x,y) + \frac{1-\sqrt{p^*}}{2} F_2(x,y), \tag{1}$$

where F_1 and F_2 are polynomials in two variables with integer coefficients. Applying the automorphism σ_j with $j \in N$ gives

$$G(x,y) = F_1(x,y) + \frac{1+\sqrt{p^*}}{2} F_2(x,y). \tag{2}$$

If $p \equiv 1 \pmod 4$, then the symmetry $F(x,y) = F(y,x)$ together with (1) imply that F_1 and F_2 are symmetric functions with integer coefficients. By the fundamental theorem of symmetric polynomials, $F_i(x,y) = H_i(x+y, xy)$ for polynomials H_1 and H_2 with integer coefficients. Then,

$$F(\alpha,\beta) = u + \frac{1-\sqrt{p}}{2} v,$$

and

$$G(\alpha,\beta) = u + \frac{1+\sqrt{p}}{2} v,$$

where $u = H_1(r,-s) \in \mathbf{Z}$ and $v = H_2(r,-s) \in \mathbf{Z}$. Then,

$$\begin{aligned} A_p &= F(\alpha,\beta)\,G(\alpha,\beta) \\ &= \left(u + \frac{1-\sqrt{p}}{2}v\right)\left(u + \frac{1+\sqrt{p}}{2}v\right) \\ &= u^2 + uv - \frac{p-1}{4}v^2. \end{aligned}$$

Consequently,

$$4A_p = (2u+v)^2 - pv^2.$$

Now assume that $p \equiv 3 \pmod 4$. From (1) and (2), we get

$$2F(x,y) = K_1(x,y) - \sqrt{-p}K_2(x,y), \tag{3}$$

and

$$2G(x,y) = K_1(x,y) + \sqrt{-p}K_2(x,y), \tag{4}$$

where $K_1(x,y) = 2F_1(x,y) + F_2(x,y)$ and $K_2(x,y) = F_2(x,y)$ have integer coefficients. This time, as $F(y,x) = -G(x,y)$, we have

$$K_1(y,x) = -K_1(x,y) \qquad \text{and} \qquad K_2(x,y) = K_2(y,x).$$

As before $v = K_2(\alpha,\beta)$ is an integer, but K_1 is an alternating function, so that

$$K_1(x,y) = (x-y)K_3(x,y),$$

where $K_3(x,y)$ is a symmetric function with integer coefficients. Therefore,

$$K_1(\alpha,\beta) = (\alpha-\beta)K_3(\alpha,\beta) = \sqrt{D}u,$$

with $u \in \mathbf{Z}$. Then

$$4A_p = (2F(\alpha,\beta))\,(2G(\alpha,\beta)) = K_1(\alpha,\beta)^2 + pK_2(\alpha,\beta)^2 = Du^2 + pv^2.$$

To complete the proof, we need to dispose of the case $p = 3$. Now

$$A_3 = \alpha^2 + \alpha\beta + \beta^2 = \frac{(\alpha-\beta)^2 + 3(\alpha+\beta)^2}{4} = \frac{D+3r^2}{4}.$$

Thus, $4A_3 = Du^2 + 3v^2$, with $u = 1$ and $v = r$.

Remark. The referee asked whether there is a quick way to compute u and v. This amounts to knowing $F(\alpha,\beta)$, which essentially means knowing $F(\alpha,\beta)/G(\alpha,\beta)$. In the case $\alpha = \beta = 1$ and $p \equiv 1 \pmod 4$, this last quantity is

$$\prod_{a=1}^{p-1} \left(1 - \zeta_p^a\right)^{\left(\frac{a}{p}\right)},$$

which by the analytic class number formula is ε^h, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{p})$ and h is the class number. For general r and s, the situation should be even harder. Hence, finding u and v amounts to solving a Pell-type equation and there are no efficient algorithms for this type of problem. The situation is perhaps easier for $p \equiv 3 \pmod 4$, since then the quadratic form is positive definite. Thus, while we cannot provide an overall formula for u and v, this is an interesting topic which deserves further investigation.

Acknowledgements

We thank the referee for comments which improved the quality of this paper.

References

[1] J. J. Alba González, P. Berrizbeitia and F. Luca, "On the formula $F_p = u^2 + pv^2$", *Internat. J. Number Theory* **11** (2015), 185–191.

[2] J. J. Alba González and F. Luca, "On the positive integers n satisfying the equation $F_n = x^2 + ny^2$", *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics*, Vol. 587 (American Mathematical Society, Providence, RI, 2013), pp. 95–109.

[3] C. Ballot and F. Luca, "On the equation $x^2 + dy^2 = F_n$", *Acta Arith.* **127** (2007), 145–155.

[4] E. Lucas, "Théorie des fonctions numériques simplement périodiques", *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[5] M. R. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, Second Edition, Springer 2004.

[6] D. Savin, "Fibonacci primes of special forms", *Notes on Number Theory and Discrete Math.* **20.2** (2014), 10–19.

Departamento de Matemáticas Pura y Aplicada, Universidad Simón Bolívar, Caracas, Venezuela
E-mail address: pberrizbeitia@gmail.com

Mathematics Research Institute, University of Exeter, Exeter, EX4 4QF, UK
E-mail address: R.J.Chapman@ex.ac.uk

School of Mathematics, University of the Witwatersrand, P. O. Wits 2050, South Africa
E-mail address: florian.luca@wits.ac.za

Departamento de Matemáticas Pura y Aplicada, Universidad Simón Bolívar, Caracas, Venezuela
E-mail address: jacob@usb.ve