CONSERVATION OF THE INTEGRALITY OF CERTAIN QUOTIENTS BY ITERATED SUBSTITUTIONS OF LUCAS NUMBERS

P. A. Picon

Abstract. If we replace k by a Lucas number, $\frac{u^k-v^k}{u-v}$, in certain integral quotients such as the binomial coefficients, the quotient remains integral. We show that this substitution may be repeated indefinitely, while preserving the integrality, for a very large class of quotients.

1. Introduction. The Lucas numbers [1] — or those of Lucas–Carmichael[1] [2] — are given by the expression $\frac{u^k-v^k}{u-v}$, where n is an integer ≥ 1, and $u+v$ and uv are rational integers which we suppose to be coprime. Thus, u and v are quadratic or rational integers, which we further assume to be both non-zero and with a ratio which is not a root of unity. The Lucas numbers are thus rational integers insofar as they are integral symmetric functions of u and v whose elementary symmetric functions $u+v$ and uv are rational integers.

The numbers have been generalized by Lehmer [3], by taking, for $n \geq 1$, $\frac{u^k-v^k}{u-v}$, if n is odd, and $\frac{u^k-v^k}{u^2-v^2}$, if n is even, with $(u+v)^2$ and uv rational coprime integers and the same restrictions for u and v: non-zero, and $\frac{u}{v}$ different from a root of unity. These are rational integers since, in the two cases, the expression are written in an integral way as functions of uv and $(u+v)^2$.

We call D_n a Lucas–Carmichael or, equally, Lehmer number. These authors show in particular two things: on the one hand[2], that the g.c.d. of D_m and D_n is D_d, where d is the g.c.d. of m and n, and, on the other hand, that if in the binomial coefficient $\frac{(m+n)!}{m!\,n!}$, and certain other integral quotients, we replace k by D_k, the quotients remain integral: it is well-known that, for example,

$$\frac{F_1F_2\cdots F_{m+n}}{F_1F_2\cdots F_m\cdot F_1F_2\cdots F_n}$$

is an integer, where F_n is the n-th Fibonacci number, the Fibonacci numbers being a special instance of the numbers D_n. These two properties are proved independently of one another.

[1]The inventor of these numbers and their principal properties is Lucas. However, Carmichael generalizes certain results and corrects some errors in an exposé, which is much more direct, and clearer at the same time.

[2]M. Ward [4] proves it once again for u and v integral

In the following, we prove again, in a more direct fashion, the property of g.c.d., by generalizing to algebraic integers. Then, we use it to show that we can repeat the substitution of n by $|D_n|$ indefinitely:

$$n \longrightarrow |D_n| \longrightarrow |D_{|D_n|}| \longrightarrow \cdots,$$

where the D are any Lucas or Lehmer numbers, while preserving the integrality, and we can do this for a very large class of quotients. For example,

$$\frac{D_1 D_2 \cdots D_{m+n}}{D_1 D_2 \cdots D_m \cdot D_1 D_2 \cdots D_n},$$

where $D = \frac{u^F - v^F}{u-v}$, is still an integer. We denote by (r, s) the positive g.c.d. of the rational integers r and s. We denote by (u) the principal ideal generated by the algebraic integer u and, for ease, we denote by (u, v) the g.c.d. of (u) and (v). We can show straight away that $(u + v, uv) = 1$ of $\big((u + v)^2, uv\big) = 1$ is the same as having $(u, v) = (1)$.

2. Property of the g.c.d.. Iterations.

Lemma. *Let u and v be two non-zero integers of an algebraic number field, whose ratio is not a root of unity. We suppoe that $(u, v) = (1)$. Then the g.c.d. of the principal ideals $\left(\frac{u^m - v^m}{u-v}\right)$ and $\left(\frac{u^n - v^n}{u-v}\right)$ is the principal ideal $\left(\frac{u^d - v^d}{u-v}\right)$, where m and n are positive integers, and $d = (m, n)$. If m is even and n is odd, then $\left(\frac{u^d - v^d}{u-v}\right)$ is still the g.c.d. of $\left(\frac{u^m - v^m}{u^2-v^2}\right)$ and $\left(\frac{u^n - v^n}{u-v}\right)$.*

Proof. We have the identity

$$v^m \left(u^{n-m} - v^{n-m}\right) = u^n - v^n - u^{n-m} \left(u^m - v^m\right),$$

with $m < n$. If $\mathbb{P}$ is a prime ideal which divides $(u^m - v^m)$ and $(u^n - v^n)$, then it also divides $(v^m)(u^{n-m} - v^{n-m})$, and thus one or the other of the two ideals. It cannot divide (v^m) since it would divide (v), and thus (u), which contradicts the fact that $(u, v) = (1)$. Also $\mathbb{P}$ divides $(u^{n-m} - v^{n-m})$ and thus also $(u^d - v^d)$, since $d = \alpha n - \beta m$ and since $(u^n - v^n)$ divides $(u^{\alpha n} - v^{\alpha n})$, as $(u^m - v^m)$ divides $(u^{\alpha m} - v^{\alpha m})$. Thus, we have

$$\left(\frac{u^m - v^m}{u - v}, \frac{u^n - v^n}{u - v}\right) = \left(\frac{u^d - v^d}{u - v}\right).$$

For the second assertion, it is sufficient to verify that

$$\left(u + v, \frac{u^n - v^n}{u - v}\right) = (1).$$

In fact, for odd n, we have

$$\frac{u^n - v^n}{u - v} = (-1)^{(n-1)/2}(uv)^{(n-1)/2} + (u + v)^2 P,$$

where P is a polynomial in uv and $(u+v)^2$, and, since a prime ideal dividing $(u+v)$ and $\left(\frac{u^n-v^n}{u-v}\right)$ would also divide (uv), we have a contradiction of $(u,v)=(1)$.

The equality $(a)=(b)$ between principal ideals is the same as saying that $a=\varepsilon b$, where ε is a unit of the number field. Since the only units of $\mathbb{Q}$ are 1 and -1, then, passing from principal ideals to numbers, we have the following proposition.

Proposition 1. *The g.c.d. of D_m and D_n is, up to sign, D_d, where d is the g.c.d. of m and n.*

And, since $D_1=1$, we have

Corollary. *If m and n are coprime, then D_m and D_n are coprime.*

With a slight abuse of notation, let us call D the map sending n to the positive integer $|D_n|$ and $D\hat{}$ the map which sends the pair (n,m) to the pair $(|D_n|,|D_m|)$. If δ denotes the operator g.c.d., Proposition 1 becomes

$$D\circ\delta=\delta\circ D\hat{}.$$

Now let us take a finite sequence of maps D, and their composition product $\mathbb{D}$, which we call an *iterated* map, or simply an *iteration*. It is immediate by recurrence that this result applies to any iteration, since:

$$D\circ D'\circ\delta=D\circ\delta\circ D'\hat{}=\delta\circ D\hat{}\circ D'\hat{}=\delta\circ(D\circ D')\hat{},$$

and we have $\mathbb{D}\circ\delta=\delta\circ\mathbb{D}\hat{}$, where $\mathbb{D}\hat{}$ is the composition product of the $D\hat{}$'s. Thus we have

Proposition 2. *The g.c.d. of $\mathbb{D}(m)$ and $\mathbb{D}(n)$ is $\mathbb{D}(d)$, where d is the g.c.d. of m and n.*

Since, for all the maps D, $D(1)=1$, we also have $\mathbb{D}(1)=1$, and the

Corollary. *If m and n are coprime, then $\mathbb{D}(m)$ and $\mathbb{D}(n)$ are coprime.*

Let $\mathbb{D}$ be an iterated map. If a is a positive integer, we call $\lambda(a)$ the smallest integer λ such that a divides $\mathbb{D}(\lambda)$ (if $\lambda(a)$ does not exist, then we take it to be infinite). We then have the following proposition.

Proposition 3. *The integer a divides $\mathbb{D}(n)$ if and only if $\lambda(a)$ divides n.*

Proof. If a divides $\mathbb{D}(\lambda(a))$, then a divides all the $\mathbb{D}(k\lambda(a))$, $k=1,2,\ldots$, as $\mathbb{D}(\lambda(a))$ divides $\mathbb{D}(k\lambda(a))$, since $\lambda(a)$ divides $k\lambda(a)$. Conversely, a divides only this sequence. In fact, if a divides $\mathbb{D}(\lambda')$, then, from Proposition 2, a also divides $\mathbb{D}(l)$, where $l=(\lambda(a),\lambda')\le\lambda(a)$; but the minimality of $\lambda(a)$ implies that $\lambda(a)\le l$. Thus $l=\lambda(a)$ and $\lambda'=k\lambda(a)$.

If F is a finite family of positive integers, let us call $\mathbb{D}(F)$ the family of positive integers $\mathbb{D}(n)$, where n runs through F, and $\#_aF$ the number of multiples of the integer a in a family F. The first part of the preceding proposition implies that $\#_a\mathbb{D}(F)\ge\#_{\lambda(a)}F$, while the second part implies the inverse inequality. Thus, we have

Corollary 1. $\#_a\mathbb{D}(F) = \#_{\lambda(a)}F$.

We can immediately obtain the following corollary.

Corollary 2. *Let us take two infinite families, F and G, of positive integers. If, for every integer $a \geq 2$, we have $\#_aF \geq \#_aG$, then, for every integer $a \geq 2$, we also have $\#_a\mathbb{D}(F) = \#_a\mathbb{D}(G)$.*

3. Application to the iteration of integral quotients. We call the q-analogue of a positive integer n the polynomial $\frac{1-q^n}{1-q}$, and we denote by F_q the family of q-analogues of a family F. We denote by $\Pi(F)$ the product of the elements of a family F. We prove in [8] the following results:

$\frac{\Pi(F_q)}{\Pi(G_q)}$ *is a polynomial if and only if, for all $a \geq 2$, $\#_aF \geq \#_aG$* (Proposition 1), and (its corollary): *If the u are homogeneous forms of the same positive degree, continuous and positive in a cone K of $\mathbb{R}^n$, then a necessary and sufficient condition for $\prod_u[u(X)]!_q^{\varepsilon_u}$, $\varepsilon_u = \pm 1$, to be a polynomial of $\mathbb{Z}[q]$, for $X \in K$, is that $\prod_u[u(X)]!^{\varepsilon_u}$ be integral, for $X \in K$.*

The notation $[x]$ denotes the integer part of x, and $n!_q$ denotes the q-factorial, i.e., $\Pi(F_q)$, if F is the family $1, 2, \ldots, n$. A cone is a subset of $\mathbb{R}^n$, invariant for positive homothety of centre O.

Since each D_n is a specialization of $\frac{1-q^n}{1-q}$, we have the following:

$$\#_aF \geq \#_aG \quad\Longleftrightarrow\quad \frac{\Pi(F_q)}{\Pi(G_q)} \in \mathbb{Z}[q] \quad\Longrightarrow\quad \frac{\Pi(F)}{\Pi(G)} \in \mathbb{N}.$$

Then Corollary 2 allows us to state the following theorem.

Theorem. *Let $\mathbb{D}$ be any iteration.*

(1) *Let F and G be two infinite families of positive integers. If $\frac{\Pi(F_q)}{\Pi(G_q)}$ is a polynomial of $\mathbb{Z}[q]$, then $\frac{\Pi(\mathbb{D}(F))}{\Pi(\mathbb{D}(G))}$ is an integer.*

(2) *Let us take a family of homogeneous forms u of the same degree > 0 on $\mathbb{R}^n$, and let K be a cone in which they are positive. If $\prod_u[u(X)]!^{\varepsilon_u}$, $\varepsilon_u = \pm 1$, is integral for $X \in K$, then*

$$\prod_u \left(\mathbb{D}(1) \cdot \mathbb{D}(2) \cdots \mathbb{D}([u(X)])\right)^{\varepsilon_u}$$

is integral for $X \in K$.

The theorem applies to all the polynomial q-analogues of quotients shown in [8], and in particular to the Young numbers. It also applies to all the quotients of homogeneous or linear forms whose integrality is shown in [5], [6] and [7].

Remark. In the first step of the iteration, we pass from $\#_aF \geq \#_aG$, which implies that $\frac{\Pi(F)}{\Pi(G)}$ is integral, to $\frac{\Pi(D(F))}{\Pi(D(G))}$, an integer, and, at the same time, we see clearly that

$\frac{\Pi(F_q)}{\Pi(G_q)} \in \mathbb{Z}[q]$. We have the same thing at each step, when we passs from an integral quotient to another integral quotient and a polynomial quotient simultaneously. At this stage, we do not need the property of the g.c.d.. It is proved, by using, as Carmichael does,

$$\frac{1-q^n}{1-q} = \prod_{d|n} \Phi_d,$$

where Φ_d is the d-th cyclotomic polynomial, and noting that, if $\#_a F \geq \#_a G$, then the family of divisors of F contains that of G. However, we cannot move onto the next stage without having $\#_a D(F) \geq \#_a D(G)$, which is proved by the property of the g.c.d., and which is thus the key to this indefinite iteration.

References

1. E. LUCAS, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240 and 289–321.
2. R. D. CARMICHAEL, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Math. **15** (1913), 30–70.
3. D. H. LEHMER, *An extended theory of Lucas' functions*, Annals of Math. **31** (1930), 419–448.
4. M. WARD, *On the number of vanishing terms in an integral cubic recurrence*, Amer. Math. Monthly **62** (1955), 155–160.
5. P. A. PICON, *Conditions d'intégrité de certains coefficients hypergéométriques. Généralisation d'un théorème de Landau*, Discrete Math. **135** (1994), 245–263.
6. P. A. PICON, *A more precise formulation of a theorem of Landau in the linear case and some applications*, European J. Combin. **15** (1994), 561–577.
7. P. A. PICON, *Sum-translation and symmetry operators and integrality of hypergeometric linear coefficients*, Internat. J. Algebra Comput. **5** (1995), 19–45.
8. P. A. PICON, *q-extension of a theorem of Landau. Integrality of affine hypergeometric coefficients and polynomiality of the q-analogues*, Internat. J. Algebra Comput. **5** (1995), 105–125.

Institut Gaspard Monge, Université de Marne-la-Vallée, 2, rue de la Butte-Verte, 93166 Noisy-le-Grande Cedex