ACTA ARITHMETICA
XCVI.4 (2001)

An extension of the Lucas theorem

by

JACQUES BOULANGER and JEAN-LUC CHABERT (Amiens)

1. Introduction. Recall Lucas' theorem [10, pp. 417–420] or [5] and [7]:

PROPOSITION 1.1. *Let p be a prime number and let*

$$n = n_0 + n_1 p + n_2 p^2 + \ldots + n_k p^k \quad \text{with } 0 \le n_i < p,$$
$$x = x_0 + x_1 p + x_2 p^2 + \ldots + x_k p^k \quad \text{with } 0 \le x_j < p.$$

Then

$$\binom{x}{n} \equiv \binom{x_0}{n_0}\binom{x_1}{n_1}\ldots\binom{x_k}{n_k} \pmod{p}.$$

This formula has been generalized by several authors (see, for instance, [8] or [9]), but all these extensions concern ordinary integers. The aim of this paper is to extend the Lucas formula by replacing $\mathbb{Z}$, or more precisely $\mathbb{Z}_{(p)}$, by a discrete valuation domain V with finite residue field. Note that the prime number p appears twice: once as a generator of the maximal ideal $p\mathbb{Z}$, and secondly as the cardinality of the residue field $\mathbb{Z}/p\mathbb{Z}$. Thus, we will replace it either by a generator t of the maximal ideal $\mathfrak{m}$ of V, or by the cardinality q of the residue field $V/\mathfrak{m}$. The integer q will then occur in the q-adic representation of the integers n, while the generator t will occur in the t-adic expansion of the elements x of V.

Now we have to replace the binomial coefficients by suitable expressions. To do this, we notice that the binomial coefficient $\binom{x}{n}$ is the value at x of the polynomial

$$\binom{X}{n} = \frac{X(X-1)\ldots(X-n+1)}{n!}.$$

It is well known that these binomial polynomials form a basis of the $\mathbb{Z}$-module

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$$

2000 *Mathematics Subject Classification*: 13F20, 11B65.

of integer-valued polynomials on $\mathbb{Z}$. We are then led to consider the ring $\mathrm{Int}(V)$ of integer-valued polynomials on V, that is,

$$\mathrm{Int}(V) = \{f \in K[X] \mid f(V) \subseteq V\},$$

where K denotes the quotient field of V. We know how to construct a basis $C_n(X)$ of the V-module $\mathrm{Int}(V)$ [1, Chap. II, §2]: we first construct a sequence $\{u_n\}_{n\in\mathbb{N}}$ of elements of V such that, for every s, any choice of q^s consecutive terms provides a complete set of residues of V mod $\mathfrak{m}^s$. Then, the following polynomials of Lagrangian type:

$$C_n(X) = \prod_{k=0}^{n-1} \frac{X - u_k}{u_n - u_k}$$

form a basis of the V-module $\mathrm{Int}(V)$. We are going to show that, for a proper choice of the sequence $\{u_n\}$, if

$$n = \sum_{i=0}^{k} n_i q^i \quad \text{and} \quad x = \sum_{j\geq 0} x_j t^j,$$

then

$$C_n(x) \equiv \prod_{i=0}^{k} C_{n_i}(x_i) \pmod{\mathfrak{m}}.$$

This generalized formula will be established in the following section. Then, in the third section, analogously to Chapman and Smith's paper about $\mathrm{Int}(\mathbb{Z})$ [4], we will use the extended formula to describe some maximal ideals of the ring $\mathrm{Int}(V)$.

2. Extension of the Lucas theorem

Hypotheses and notations. Let V be a discrete valuation domain with finite residue field. Denote by K the quotient field of V, by v the corresponding valuation of K, by $\mathfrak{m}$ the maximal ideal of V, and by q the cardinality of the residue field $V/\mathfrak{m}$. We denote by $\widehat{K}$, $\widehat{V}$, and $\widehat{\mathfrak{m}}$ the completions of K, V, and $\mathfrak{m}$ with respect to the $\mathfrak{m}$-adic topology and we still denote by v the extension of v to $\widehat{K}$.

The construction. We choose a generator t of $\mathfrak{m}$ and a set $U = \{u_0 = 0, u_1, \ldots, u_{q-1}\}$ of representatives of V modulo $\mathfrak{m}$. It is well known that each element x of $\widehat{V}$ has a unique t-adic expansion (see, for instance, [2, Chap. II, §7])

$$x = \sum_{j=0}^{\infty} x_j t^j \quad \text{with } x_j \in U \text{ for each } j \in \mathbb{N}.$$

We now construct a sequence $\{u_n\}_{n\in\mathbb{N}}$ of elements of V which will replace the sequence of nonnegative integers. Taking q as the basis of the numeration, that is, writing every positive integer n in the form

$$n = n_0 + n_1 q + n_2 q^2 + \ldots + n_k q^k \quad \text{with } 0 \le n_i < q \text{ for each } i \in \{0, \ldots, k\},$$

we extend the sequence $\{u_j\}_{0\le j<q}$ in the following way:

$$u_n = u_{n_0} + u_{n_1} t + u_{n_2} t^2 + \ldots + u_{n_k} t^k.$$

We then replace the binomial polynomials

$$\binom{X}{n} = \frac{X(X-1)(X-2)\ldots(X-n+1)}{n!}$$

by the polynomials

$$C_n(X) = \prod_{k=0}^{n-1} \frac{X-u_k}{u_n-u_k} \quad \text{with } C_0 = 1,$$

and we recall:

PROPOSITION 2.1 ([1, Theorem II.2.7]). *The polynomials $C_n(X)$ form a basis of the V-module* $\mathrm{Int}(V)$.

THEOREM 2.2 (generalized Lucas formula). *If*

$$n = n_0 + n_1 q + \ldots + n_k q^k$$

is the q-adic expansion of a positive integer n, and if

$$x = x_0 + x_1 t + \ldots + x_j t^j + \ldots$$

is the t-adic expansion of an element x of $\widehat{V}$, then

$$C_n(x) \equiv C_{n_0}(x_0) C_{n_1}(x_1) \ldots C_{n_k}(x_k) \pmod{\widehat{\mathfrak{m}}}.$$

We first note that the above theorem is equivalent to the following proposition:

PROPOSITION 2.3. *Let $n_0 \in \{0, 1, \ldots, q-1\}$ and $x_0 \in \{u_0 = 0, u_1, \ldots \ldots, u_{q-1}\}$. Then, for every $m \in \mathbb{N}$ and every $y \in \widehat{V}$,*

$$C_{n_0+qm}(x_0 + ty) \equiv C_{n_0}(x_0) C_m(y) \pmod{\widehat{\mathfrak{m}}}.$$

Proof of the equivalence. Theorem 2.2 obviously implies Proposition 2.3. Let us prove the converse implication. Let $n = n_0 + n_1 q + \ldots + n_k q^k \in \mathbb{N}$ and $x = x_0 + x_1 t + \ldots + x_j t^j + \ldots \in \widehat{V}$. Write $n = n_0 + q m_1$ and $x = x_0 + t y_1$. It follows from Proposition 2.3 that

$$C_n(x) \equiv C_{n_0}(x_0) C_{m_1}(y_1) \pmod{\widehat{\mathfrak{m}}}.$$

Now writing $m_1 = n_1 + q m_2$ and $y_1 = x_1 + t y_2$, analogously we have

$$C_{m_1}(y_1) \equiv C_{n_1}(x_1) C_{m_2}(y_2) \pmod{\widehat{\mathfrak{m}}}.$$

And so on, until we come to

$$C_{m_{k-1}}(y_{k-1}) \equiv C_{n_{k-1}}(x_{k-1})C_{n_k}(y_k) \pmod{\widehat{\mathfrak{m}}}.$$

To conclude we just have to notice that

$$n_k = n_k + q \cdot 0 \quad \text{and} \quad y_k = x_k + ty_{k+1};$$

thus we have

$$C_{n_k}(y_k) \equiv C_{n_k}(x_k) \cdot C_0(y_{k+1}) = C_{n_k}(x_k) \pmod{\widehat{\mathfrak{m}}}. \ ■$$

Proof of Proposition 2.3. First note that our choice of the sequence $\{u_n\}_{n\in\mathbb{N}}$ implies that, for each $h, k \in \mathbb{N}$ with $0 \le k < q$, one has $u_{hq+k} = u_k + tu_h$. By hypothesis, $n = n_0 + qm$ where $0 \le n_0 < q$ and $x = x_0 + ty$ where $x_0 = u_s$ for some $s \in \{0, \dots, q-1\}$. Hence, in particular, $u_n = u_{n_0} + tu_m$ and $u_n - u_{qm+l} = u_{n_0} - u_l$ for $0 \le l < q$. Then

$$C_n(x) = \prod_{k=0}^{n-1} \frac{x - u_k}{u_n - u_k} = \prod_{k=0}^{qm-1} \frac{x - u_k}{u_n - u_k} \cdot \prod_{l=0}^{n_0-1} \frac{x - u_{qm+l}}{u_n - u_{qm+l}} = A \cdot B.$$

The second factor B is equal to

$$\prod_{l=0}^{n_0-1} \frac{x - u_{qm+l}}{u_{n_0} - u_l},$$

and hence is congruent modulo $\widehat{\mathfrak{m}}$ to

$$C_{n_0}(x_0) = \prod_{l=0}^{n_0-1} \frac{x_0 - u_l}{u_{n_0} - u_l}$$

because:

- the denominators of both fractions are equal and invertible,
- the numerators are congruent modulo $\widehat{\mathfrak{m}}$ since

$$x - u_{qm+l} = x_0 - u_l + t(y - u_m).$$

If we prove that

$$A = \prod_{k=0}^{qm-1} \frac{x - u_k}{u_n - u_k} \equiv C_m(y) \pmod{\widehat{\mathfrak{m}}},$$

then in particular A and B belong to $\widehat{V}$, and hence, $A \cdot B \equiv C_m(y) \cdot C_{n_0}(x_0)$ $\pmod{\widehat{\mathfrak{m}}}$. Writing

$$A = \prod_{h=0}^{m-1} \prod_{k=0}^{q-1} \frac{x - u_{qh+k}}{u_n - u_{qh+k}} = \prod_{h=0}^{m-1} \prod_{k=0}^{q-1} \frac{(u_s + ty) - (u_k + tu_h)}{(u_{n_0} - u_k) + t(u_m - u_h)},$$

we consider the k's equal to s in the numerators and the k's equal to n_0 in the denominators:

$$A = \prod_{h=0}^{m-1} \frac{y-u_h}{u_m-u_h} \cdot \prod_{h=0}^{m-1} \frac{\prod_{1\le k<q,\, k\neq s}[(u_s-u_k)+t(y-u_h)]}{\prod_{0\le k<q,\, k\neq n_0}[(u_{n_0}-u_k)+t(u_m-u_h)]}.$$

Write

$$A = E \cdot \prod_{h=0}^{m-1} \frac{N_h}{D_h}.$$

The first factor E is exactly $C_m(y)$. Consequently, it suffices to prove that the second factor is congruent to 1 modulo $\widehat{\mathfrak{m}}$, and hence that all the quotients N_h/D_h are congruent to 1 modulo $\widehat{\mathfrak{m}}$. Of course,

$$N_h = \prod_{1\le k<q,\, k\neq s} [(u_s-u_k)+t(y-u_h)] \equiv \prod_{1\le k<q,\, k\neq s} (u_s-u_k) \pmod{\widehat{\mathfrak{m}}},$$

$$D_h = \prod_{0\le k<q,\, k\neq n_0} [(u_{n_0}-u_k)+t(u_m-u_h)] \equiv \prod_{1\le k<q,\, k\neq n_0} (u_{n_0}-u_k) \pmod{\widehat{\mathfrak{m}}},$$

and the last terms are congruent to -1 modulo $\mathfrak{m}$. This ends the proof. ■

REMARK 2.4. In the previous proof we have used the fact that $u_0 = 0$. We know that, whatever the choice of $u_0 \in V$, the polynomials $C_n(X)$ form a basis of the V-module $\mathrm{Int}(V)$. Nevertheless, if the generalized Lucas formula holds, then necessarily $u_0 = 0$. Let us prove it. Assuming that $u_0 \neq 0$, we may consider the element $x = u_0/(1-t)$ whose t-adic expansion is

$$x = \frac{u_0}{1-t} = u_0 + u_0 t + u_0 t^2 + \ldots + u_0 t^n + \ldots$$

Let $h \in \mathbb{N} \setminus \{0\}$ be such that $v(tu_0) \ge h$. It follows from the Lucas formula that

$$C_{q^h}\left(\frac{u_0}{1-t}\right) \equiv C_0(u_0)^h \cdot C_1(u_0) \pmod{\widehat{\mathfrak{m}}},$$

since $q^h = 0\cdot 1 + 0 \cdot q + \ldots + 1 \cdot q^h$. Obviously, $C_0(u_0) = 1$ and $C_1(u_0) = 0$. Consequently, $v(C_{q^h}(x)) > 0$. On the other hand, $v(x-u_0) = v(tu_0) \ge h$; it then follows from Lemma 2.5 below that

$$v(C_{q^h}(x)) = v(x-u_0) - h.$$

Thus, we have just proved that $v(tu_0) \ge h$ implies $v(tu_0) > h$. This is a contradiction with the assumption that $u_0 \neq 0$.

LEMMA 2.5 ([3, Lemme 2]). *For every $h \in \mathbb{N}$ and every $x \in \widehat{V}$,*

$$v(C_{q^h}(x)) = -h + \sup_{0\le k<q^h} v(x-u_k).$$

In particular, if $v(x-u_{k_0}) \ge h$ for some k_0 such that $0 \le k_0 < q^h$, then

$$v(C_{q^h}(x)) = v(x-u_{k_0}) - h.$$

It is known [1, II.2.4] that the valuation of the denominator of $C_n(X)$ is

$$v\Big(\prod_{k=0}^{n-1}(u_n-u_k)\Big)=w_q(n)=\sum_{k>0}\Big[\frac{n}{q^k}\Big]$$

where $[z]$ denotes the integer part of z. Thus, if we replace the denominator of $C_n(X)$ by $(-t)^{-w_q(n)}$, we obtain another sequence of polynomials

$$\mathit{\Gamma}_n(X)=(-t)^{-w_q(n)}\prod_{k=0}^{n-1}(X-u_k)$$

which form a basis of the V-module $\mathrm{Int}(V)$ [1, II.2.10].

PROPOSITION 2.6. *The generalized Lucas formula holds for the polynomials $\mathit{\Gamma}_n(X)$, that is, if $n=\sum_{0\le i\le k}n_iq^i$ and $x=\sum_{j\ge0}x_jt^j$, then*

$$\mathit{\Gamma}_n(x)\equiv\mathit{\Gamma}_{n_0}(x_0)\mathit{\Gamma}_{n_1}(x_1)\dots\mathit{\Gamma}_{n_k}(x_k)\pmod{\widehat{\mathfrak{m}}}.$$

Proof. Of course, it suffices to prove that

$$\mathit{\Gamma}_{n_0+qm}(x_0+ty)\equiv\mathit{\Gamma}_{n_0}(x_0)\mathit{\Gamma}_m(y).$$

The proof of this last assertion is similar to that of Proposition 2.3. We first notice that $w_q(n)=m+w_q(m)$. Then $\mathit{\Gamma}_n(x)=A\cdot B$ where

$$A=(-t)^{-w_q(n)}\prod_{k=0}^{qm-1}(x-u_k)\quad\text{and}\quad B=\prod_{l=0}^{n_0-1}(x-u_{qm+l}).$$

Obviously,

$$B\equiv\prod_{l=0}^{n_0-1}(x_0-u_l)=\mathit{\Gamma}_{n_0}(x_0)\pmod{\widehat{\mathfrak{m}}}.$$

On the other hand,

$$A=(-t)^{-w_q(n)}\prod_{h=0}^{m-1}\prod_{k=0}^{q-1}(x-u_{qh+k})=(-t)^{-w_q(n)}\prod_{h=0}^{m-1}\prod_{k=0}^{q-1}[(x_0-u_k)+t(y-u_h)].$$

Let $s\in\{0,\dots,q-1\}$ be such that $x_0=u_s$. Then

$$A=(-1)^m\cdot(-t)^{-w_q(m)}\prod_{h=0}^{m-1}(y-u_h)\cdot\prod_{h=0}^{m-1}\prod_{0\le k<q,\,k\ne s}[(x_0-u_k)+t(y-u_h)].$$

The second factor is exacly $\mathit{\Gamma}_m(y)$, while the third is congruent to $(-1)^m$ modulo $\widehat{\mathfrak{m}}$. ■

Remark 2.4 still holds for the $\mathit{\Gamma}_n(X)$'s since $\mathit{\Gamma}_0(X)=1$ and $\mathit{\Gamma}_1(u_0)=0$; if the generalized Lucas formula holds for the polynomials $\mathit{\Gamma}_n(X)$, then necessarily $u_0=0$.

REMARK 2.7. There is another classical basis of $\mathrm{Int}(V)$: the basis formed by the Fermat polynomials $F_n(X)$ (see [6], [1, §II.2], or [11]). Recall that

$$F_0 = 1, \quad F_1 = X, \quad F_q = \frac{X - X^q}{t}, \quad F_{q^{h+1}} = F_q(F_{q^h}),$$

and

$$F_n = \prod_{j=0}^{k} (F_{q^j})^{n_j} \quad \text{for } n = n_0 + n_1 q + \ldots + n_k q^k.$$

We are going to see that the Lucas formula may hold for the first indices n, but cannot hold for every n, in particular for $n = q^q$.

Let $\zeta_0 = 0, \zeta_1, \ldots, \zeta_{q-1}$ be the roots of $X - X^q = 0$ in $\widehat{V}$ and assume that $u_0 = 0, u_1, \ldots, u_{q-1} \in V$ are such that $u_i \equiv \zeta_i \pmod{t^2 \widehat{V}}$. It is then easy to prove that, for $n < q^2$,

$$F_{n_0 + n_1 q}\Big(\sum_j x_j t^j\Big) \equiv x_0^{n_0} x_1^{n_1} \pmod{t\widehat{V}}.$$

Before proving that the formula cannot hold for $n = q^q$, we may notice that there is some choice for $F_1, \ldots, F_{q-1}$: they just have to be polynomials in $V[X]$ which together with the polynomial 1 form a basis of the V-module of polynomials in $V[X]$ whose degree is $< q$. But, for $i = 0, 1, \ldots, q-1$, we have $F_q(u_i t) \equiv u_i \pmod{tV}$, and hence, if the Lucas formula holds, we have $F_1(u_i) \equiv u_i \pmod{tV}$, that is,

$$F_1(X) \equiv X \pmod{tV[X]}$$

since $\deg(F_1) < q$.

Now, note that, if $v(x) > 0$, then $v(F_q(x)) = v(x) - 1$. Then

$$F_q(t) = 1 - t^{q-1}, \qquad F_{q^2}(t) \equiv -t^{q-2} \pmod{t^{q-1} V};$$

consequently, $v(F_{q^q}(t)) = 0$ even if $q = 2$. But, the Lucas formula implies

$$F_{q^q}(t) \equiv F_1(0) \equiv 0 \pmod{tV}.$$

This is a contradiction.

The characterization of the bases of $\mathrm{Int}(V)$ for which the Lucas formula holds thus deserves to be studied.

3. Application to maximal ideals of $\mathrm{Int}(V)$**.** Recall the fiber of $\mathrm{Int}(V)$ over $\mathfrak{m}$:

PROPOSITION 3.1 ([3, Théorème 1] or [1, V.2.3]). *There is a one-to-one correspondence between the completion $\widehat{V}$ of V and the set of prime ideals of* $\mathrm{Int}(V)$ *lying over* $\mathfrak{m}$:

$$x \in \widehat{V} \mapsto \mathfrak{m}_x = \{f \in \mathrm{Int}(V) \mid f(x) \in \widehat{\mathfrak{m}}\} \in \max(\mathrm{Int}(V)).$$

Following Chapman and Smith [4], we are going to consider the polynomials $C_n(X)$ which belong to these maximal ideals $\mathfrak{m}_x$.

Proposition 3.2. *With the previous notation, let* $n = n_0 + n_1 q + \ldots + n_k q^k$ *be a positive integer and* $x = \sum_{j\geq 0} x_j t^j \in \widehat{V}$. *Then* C_n *belongs to* $\mathfrak{m}_x$ *if and only if there is some index* j *such that* $x_j = u_{\nu(x,j)}$ *with* $\nu(x,j) < n_j$.

Proof. By definition, C_n belongs to $\mathfrak{m}_x$ if and only if $C_n(x)$ belongs to $\widehat{\mathfrak{m}}$. It follows from the Lucas formula that

$$C_n(x) \equiv C_{n_0}(x_0) C_{n_1}(x_1) \ldots C_{n_k}(x_k) \pmod{\widehat{\mathfrak{m}}},$$

and hence, that $C_n \in \mathfrak{m}_x$ if and only if there is some $j \in \{0, \ldots, k\}$ such that

$$C_{n_j}(x_j) = \prod_{k=0}^{n_j - 1} (x_j - u_k) \in \mathfrak{m}.$$

This last assertion means that $x_j \in \{u_0, \ldots, u_{n_j - 1}\}$, that is, $x_j = u_{\nu(x,j)}$ with $\nu(x,j) < n_j$. ■

Remark 3.3. The previous proposition could be used to prove that if $x \neq y$, then $\mathfrak{m}_x \neq \mathfrak{m}_y$: if $x \neq y$, there is some $j \geq 0$ such that $x_j \neq y_j$, and hence, such that $\nu(x,j) \neq \nu(y,j)$. Assume that $\nu(x,j) < \nu(y,j)$ and let $n = \nu(y,j) q^j$. Then $C_n \in \mathfrak{m}_x$ while $C_n \notin \mathfrak{m}_y$.

Corollary 3.4. *Let*

$$z = \frac{u_{q-1}}{1-t} = u_{q-1} + u_{q-1} t + \ldots + u_{q-1} t^n + \ldots$$

Then $\mathfrak{m}_z$ *is the unique maximal ideal of* $\mathrm{Int}(V)$ *lying over* $\mathfrak{m}$ *which does not contain any polynomial* C_n.

On the other hand, the ideal $\mathfrak{m}_0$ contains all the C_n for $n > 0$.

Proposition 3.5. *Let* $x = \sum_{j \geq 0} x_j t^j \in \widehat{V}$ *and, for each* $n > 0$, *let*

$$y_n = \prod_{i=0}^{[\log n / \log q]} C_{n_i}(x_i) \in V.$$

Then:

(1) $\{1, C_1(X) - y_1, \ldots, C_n(X) - y_n, \ldots\}$ *is a basis of the* V*-module* $\mathrm{Int}(V)$.
(2) $\{t, C_1(X) - y_1, \ldots, C_n(X) - y_n, \ldots\}$ *is a basis of the* V*-module* $\mathfrak{m}_x$.

Proof. (1) $\{C_n - y_n\}$ is a basis of $\mathrm{Int}(V)$ because $\deg(C_n - y_n) = \deg(C_n) = n$ and, for $n \geq 1$, $C_n - y_n$ and C_n have the same leading coefficient.

(2) Let $f \in \mathfrak{m}_x$. It follows from (1) that $f = a_0 + \sum_{n \geq 1} a_n (C_n - y_n)$ with $a_n \in V$. By construction and the Lucas formula, $C_n - y_n \in \mathfrak{m}_x$. Consequently, $a_0 = f - \sum_{n\geq 1} a_n (C_n - y_n)$ belongs to $\mathfrak{m}_x \cap V = \mathfrak{m} = tV$. ■

PROPOSITION 3.6. *For each $n \in \mathbb{N}$, the ideal $\mathfrak{m}_{u_n}$ is generated by the polynomials*

$$1 + (t-1)C_n \quad \textit{and} \quad C_m \textit{ for } m > n.$$

Proof. It follows from Proposition 3.2 that C_m belongs to $\mathfrak{m}_{u_n}$ for every $m > n$. Moreover, $1 + (t-1)C_n$ also belongs to $\mathfrak{m}_{u_n}$ since $C_n(u_n) = 1$. Conversely, let f be in $\mathfrak{m}_{u_n}$. Then $f(u_n) = tb$ with $b \in V$. We may find elements $a_m \in V$ such that the polynomial $g = \sum_{m=0}^{n} a_m C_m$ satisfies

$$g(u_m) = f(u_m) \quad \text{for } 0 \le m < n, \quad \text{and} \quad g(u_n) = b,$$

because the a_m's may be computed recursively:

$$a_m = f(u_m) - \sum_{k=0}^{m-1} a_k C_k(u_m) \quad \text{for } 0 \le m \le n \quad \text{and} \quad a_n = b - \sum_{k=0}^{n-1} a_k C_k(u_n).$$

Now, consider the polynomial $h = f - g[1 + (t-1)C_n]$. One has $h(u_m) = 0$ for $0 \le m \le n$. Consequently, $h = \sum_{m>n} b_m C_m$ for some $b_m \in V$. Thus,

$$f = g[1 + (t-1)C_n] + \sum_{m>n} b_m C_m,$$

that is, the polynomials $1 + (t-1)C_n$ and C_m, for $m > n$, generate $\mathfrak{m}_{u_n}$. ■

For instance,

$$t = [t - (t-1)C_n][1 + (t-1)C_n] + \sum_{m=n+1}^{2(n+1)} b_m C_m.$$

We may improve the previous proposition by noticing that, if $q^h \le m < q^{h+1}$, then C_m is a multiple of C_{q^h} in $\mathrm{Int}(V)$.

We may also use the proposition to obtain generators of a maximal ideal $\mathfrak{m}_x$ whatever $x \in \widehat{V}$: if x is not zero, then $v(x) = h$ and we choose $u_1 = x/t^h$ (which may belong to $\widehat{V}$ and not V). For such a choice, $x = u_n$ with $n = q^h$.

COROLLARY 3.7. *Let x be a nonzero element of $\widehat{V}$, let $v(x) = h$, and assume that $u_1 = x/t^h$. Then the ideal $\mathfrak{m}_x$ is generated by the polynomials*

$$1 + (t-1)C_{q^h} \quad \textit{and} \quad C_m \textit{ for } m > q^h.$$

Of course, we obtain the known results on the binomial coefficients and the binomial polynomials if we replace V by $\mathbb{Z}_{(p)}$ for some prime number p, t and q by p, u_n by n, and $C_n(X)$ by $\binom{X}{n} = X(X-1)\ldots(X-n+1)/n!$.

REMARK 3.8. Note that there are other nonzero prime ideals of $\mathrm{Int}(V)$, those lying over the ideal (0) of V, that is, the ideals $\mathfrak{P}_g = gK[X] \cap \mathrm{Int}(V)$ where g is a polynomial irreducible in $K[X]$. Moreover, the ideal $\mathfrak{P}_g$ is maximal if and only if g has no root in $\widehat{V}$ [1, Proposition V.2.5]. We may first notice that $\mathfrak{P}_g$ contains some polynomial C_m if and only if $g = X - u_n$ for some $n < m$ (and hence, $\mathfrak{P}_g$ is not maximal).

Let us fix a nonnegative integer n. We easily see that:

(a) $\{1, C_1(X) - C_1(u_n), \ldots, C_n(X) - C_n(u_n), C_{n+1}(X), \ldots, C_m(X), \ldots\}$ is a basis of the V-module $\mathrm{Int}(V)$,

(b) $\{C_1(X) - C_1(u_n), \ldots, C_n(X) - C_n(u_n), C_{n+1}(X), \ldots, C_m(X), \ldots\}$ is a basis of the V-module $\mathfrak{P}_{X-u_n}$.

Moreover, in the same line as Proposition 3.6:

(c) The ideal $\mathfrak{P}_{X-u_n}$ is generated by the polynomials $1 - C_n(X)$ and $C_m(X)$ for $m > n$ (because, for each $f \in \mathfrak{P}_{X-u_n}$, the value of fC_n for $X = u_0, u_1, \ldots, u_n$ is 0).

References

[1] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys Monogr. 48, Providence, 1997.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[3] J.-L. Chabert, *Anneaux de "polynômes à valeurs entières" et anneaux de Fatou*, Bull. Soc. Math. France 99 (1971), 273–283.

[4] S. T. Chapman and W. W. Smith, *Generators of maximal ideals in the ring of integer-valued polynomials*, Rocky Mountain J. Math. 28 (1998), 95–105.

[5] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.

[6] G. Gerboud, *Construction, sur un anneau de Dedekind, d'une base régulière de polynômes à valeurs entières*, Manuscripta Math. 65 (1989), 167–179.

[7] A. Granville, *Arithmetic properties of binomial coefficients. I: Binomial coefficients modulo prime powers*, in: CMS Conf. Proc. 20, Amer. Math. Soc., Providence, 1997, 253–276.

[8] J. M. Holte, *A Lucas-type theorem for fibonomial-coefficient residues*, Fibonacci Quart. 32 (1994), 60–68.

[9] D. E. Knuth and H. S. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. 396 (1989), 212–219.

[10] E. Lucas, *Théorie des nombres*, 1878; reprint, Librairie Blanchard, Paris, 1961.

[11] K. Tateyama, *Continuous functions on discrete valuation rings*, J. Number Theory 75 (1999), 23–33.

LAMFA, UPRES-A 6119
Faculté de Mathématiques et d'Informatique
Université de Picardie
33 rue Saint Leu
80039 Amiens, France
E-mail: jacques-j.boulanger@wanadoo.fr
jlchaber@worldnet.fr

Received on 8.7.1999 (3646)