in: Applications of Fibonacci Numbers, Vol. 7 (Graz 1996 Conf.)
G. E. Bergum, A. N. Philippou, A. F. Horadam (eds.), Kluwer 1998, pp 133 – 144

BINOMIAL COEFFICIENTS GENERALIZED WITH RESPECT TO A DISCRETE VALUATION

Sophie Frisch

1. Introduction. There is a fine Theorem of Kummer on the power to which a prime appears in the prime factorization of a binomial coefficient:

Theorem. (Kummer [10]) *If p is a prime, then the exact power of p dividing the binomial coefficient $\binom{n}{k}$ is equal to the number of carries that occur in the addition of k and $n-k$ in base p arithmetic.*

One objective of this paper is to show an analogue of this result for a certain generalization of the binomial coefficients that arises naturally in the study of integer-valued polynomials. Recall that a polynomial with coefficients in the quotient field K of an integral domain D is called integer-valued if $f(d) \in D$ for all $d \in D$. The starting point of this generalization is the following well known fact.

Fact 1. (folklore) *Let $(x)_n = x(x-1)\dots(x-n+1)$, $(x)_0 = 1$. The binomial polynomials*

$$\binom{x}{n} = \frac{(x)_n}{n!} \quad (n \in \mathbb{N}_0)$$

form a basis of the free $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$.

To be able to generalize the falling factorials $(x)_n = x(x-1)\dots(x-n+1)$, we need a sequence with nice distribution properties with respect to a discrete valuation to take the place of the sequence of natural numbers.

Before we make this precise, we state the second objective of this paper, namely to show that in certain cases, in particular when R is the ring of algebraic integers in a number field, these sequences can be chosen to enumerate R bijectively. For this, we introduce $\mathbb{Z}$-bases with special properties with respect to a prime $p \in \mathbb{Z}$ for the ring of algebraic integers in a number field in section 5.

2. Definitions. Integer-valued polynomials are much studied objects; we mention only the seminal work by Pólya [16] and Ostrowski [15], and, as more recent examples, the papers by Cahen [1, 2], Chabert [3], McQuillan [13, 14] and Gilmer, Heinzer and Lantz [6]. We use the common notation of $\mathrm{Int}(R, D)$ for $\{f \in K[x] \mid f(R) \subseteq D\}$, where R is

a subset of the quotient field K of an integral domain D, and $\mathrm{Int}(D)$ for $\mathrm{Int}(D, D)$. The technique of constructing integer-valued polynomials by replacing the natural numbers in the definition of the binomial polynomials by a specially chosen sequence of ring elements goes back to Pólya [16].
We first define sequences in arbitrary commutative rings. (We will specialize to discrete valuation rings later.) All (finite or infinite) sequences are indexed by an initial segment $\mathcal{N}$ of $\mathbb{N} = \{1, 2, \ldots\}$ or $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and quantifiers over indices of such a sequence are always assumed to range over precisely the index-set.

Definition. *For a set $\mathcal{I}$ of ideals in a commutative ring R we define an $\mathcal{I}$-sequence in R to be a sequence (a_n) of elements in R with the property*

$$\forall I \in \mathcal{I} \quad \forall n, m \qquad \big(a_n \equiv a_m \mod I \quad \Longleftrightarrow \quad [R:I] \bigm| n-m\big).$$

(Any infinite $[R{:}I]$ we regard as dividing 0, but no other integer.) We define a homogeneous $\mathcal{I}$-sequence to be one with the additional property

$$\forall I \in \mathcal{I} \quad \forall n \geq 1 \qquad \big(a_n \in I \iff [R:I] \bigm| n\big).$$

Note that every $\mathcal{I}$-sequence with $a_0 = 0$ is homogeneous. Also note that a sequence in R is an $\mathcal{I}$-sequence if and only if every $[R:I]$ consecutive elements form a complete system of residues mod I for every $I \in \mathcal{I}$ of finite index, and the elements of the sequence are pairwise incongruent modulo every $I \in \mathcal{I}$ of infinite index.

It is not hard to see [4, Proposition 2.1] that $\mathcal{I}$-sequences exist for every descending chain of ideals $\mathcal{I} = \{I_n \mid n \in \mathbb{N}\}$, $I_{n+1} \subseteq I_n$, in a commutative ring R. We can therefore count on having an $\mathcal{I}$-sequence with respect to the set $\mathcal{I}$ of all ideals of R, whenever it forms a descending chain. This is our motivation for turning to discrete valuation rings.

Recall that a discrete valuation on a field K is a function v from $K \setminus \{0\}$ onto $\mathbb{Z}$ (supplemented by the convention $v(0) = \infty$) satisfying $v(ab) = v(a) + v(b)$ and $v(a+b) \geq \min(v(a), v(b))$. A discrete valuation ring is a ring $R_v = \{a \in K \mid v(a) \geq 0\}$, where v is a discrete valuation on K. It is a local ring with maximal ideal $M_v = \{a \in K \mid v(a) > 0\}$ (see, e.g. [12]).

For an important class of rings including all Dedekind rings and all unique factorization domains, R is the intersection of a family of discrete valuation rings in its quotient field, $R = \bigcap_{v \in \mathcal{V}} R_v$. For Dedekind rings, the relevant discrete valuation rings are the localizations at maximal ideals, for UFDs the localizations at principal prime ideals. One can then study $\mathrm{Int}(R) = \bigcap_{v \in \mathcal{V}} \mathrm{Int}(R, R_v)$ by first considering each $\mathrm{Int}(R, R_v)$ individually, which we will do here, and then combining the information to obtain results on $\mathrm{Int}(R)$, which we will omit, since the combinatorial properties we are interested in only appear in $\mathrm{Int}(R, R_v)$.

If R is an infinite subring of a discrete valuation ring, there is a straightforward generalization (defined below) of the binomial polynomials. They form a basis of the R_v-module $\mathrm{Int}(R, R_v)$ (cf. [4], Theorem 2.8).

Definition. *If R is an infinite subring of a discrete valuation ring R_v, we define a v-sequence for R to be an $\mathcal{I}$-sequence with $\mathcal{I} = \{{M_v}^n \cap R \mid n \in \mathbb{N}\}$. In other words,*

$(a_n)_{n\in\mathcal{N}} \subseteq R$ is a v-sequence for R if and only if for all $n \in \mathbb{N}$ and all $i,\ j \in \mathcal{N}$,

$$v(a_i - a_j) \geq n \qquad \Longleftrightarrow \qquad [R : {M_v}^n \cap R] \bigm| i - j\ .$$

If $[R\!:\!{M_v}^n \cap R]$ is infinite, the elements of a v-sequence must be pairwise incongruent mod ${M_v}^n \cap R$.

Notation. *From now on, R_v will be a discrete valuation ring (with value group $\mathbb{Z}$ and $v(0) = \infty$), M_v its maximal ideal, K its quotient field and R (unless otherwise specified) an infinite subring of R_v. For brevity, we write P_n for ${M_v}^n \cap R$, from this point on.*

Note that since R is infinite and by the Krull Intersection Theorem $\bigcap_{n=0}^{\infty} P^n = (0)$, the indices $[R : P_n]$ grow arbitrarily large or are infinite from some n on.

Definition. *The falling factorials with respect to a v-sequence $(a_n)_{n\geq 0}$ are*

$$\langle x\rangle_n = (x - a_0)(x - a_1)\ldots(x - a_{n-1})$$

and the binomial polynomials constructed from the v-sequence $(a_n)_{n\geq 0}$ are

$$b_0 = 1 \qquad \text{and} \qquad b_n(x) = \frac{\langle x\rangle_n}{\langle a_n\rangle_n} \quad \text{for } n > 0.$$

These binomial polynomials were introduced in [4]. They generalize a construction of Pólya [16] that has also been employed by Cahen [2], Gunji and McQuillan [7, 13] and others.

If $R = \mathbb{Z}$, p is a prime and v_p is p-adic valuation, then the classical v_p-sequence for $\mathbb{Z}$ is $a_n = n$. The corresponding binomial polynomials are $b_k(x) = \binom{x}{k}$, and $b_k(a_n) = \binom{n}{k}$. Therefore, if (a_n) is a v-sequence and b_k is the binomial polynomial of degree k constructed from it, we may regard $b_k(a_n)$ as a generalization of $\binom{n}{k}$.

3. A carry theorem. As before, R is an infinite subring of a discrete valuation ring R_v and $P_n = {M_v}^n \cap R$. For $j,\ k \in \mathbb{N}_0$, let $r_j(k)$ be the remainder of k under integral division by $[R : P_j]$ if $[R : P_j]$ is finite, and $r_j(k) = k$ if $[R : P_j]$ is infinite.

Lemma 1. *Let $(a_n)_{n=0}^{N}$ be a v-sequence for R and $(b_n)_{n=0}^{N}$ the binomial polynomials constructed from it. Then for all $r \in R$ and all $k = 0, \ldots, N$,*

$$v\big(b_k(r)\big) = \big|\{j \geq 1 \mid \text{for some } l < r_j(k),\ \ r \equiv a_l \mod P_j\}\big|$$

and, in particular, $b_k \in \operatorname{Int}(R, R_v)$.

Proof. $v\big(b_k(r)\big) = v\big(\langle r\rangle_k\big) - v\big(\langle a_k\rangle_k\big)$. For any $s \in R$, $v\big(\langle s\rangle_k\big) = \sum_{i=0}^{k-1} v(s - a_i)$, so

$$v\big(\langle s\rangle_k\big) = \sum_{j\geq 1}\big|\{i \mid 0 \leq i < k,\ v(s - a_i) \geq j\}\big| = \sum_{j\geq 1}\big|\{i \mid 0 \leq i < k,\ s \equiv a_i \bmod P_j\}\big|.$$

Since every $[R\!:\!P_j]$ consecutive terms of a v-sequence form a complete set of representatives mod P_j, $\big|\{i \mid 0 \leq i < k,\ s \equiv a_i \bmod P_j\}\big|$ is either $\left[\frac{k}{[R:P_j]}\right]$ or $\left[\frac{k}{[R:P_j]}\right] + 1$. The extra "1" appears for each j such that $s \equiv a_i \mod P_j$ for some i with $0 \leq i < r_j(k)$, and never appears at all if $s = a_k$. $\square$

We now introduce the number system associated to the valuation v that will appear in our generalization of Kummer's theorem. We call it v-ary number system but note that it depends not only on v, but also on the subring R of R_v. It is the Cantor (or mixed-radix) number system to the basis $b_n = [R : P_n]$, $0 \le n < \infty$, cf. [8] 192 ff. Since the indices $[R:P_n]$ either grow arbitrarily large while remaining finite (the non-degenerate case of our number system) or are finite at first, at least for $P_0 = R$, and infinite from some n on (the degenerate case), every $n \in \mathbb{N}_0$ has a unique representation $n = \sum_{l=0}^{\infty} \varepsilon_l(n)[R : P_l]$, with $0 \le \varepsilon_l(n) < [P_l : P_{l+1}]$. (We use the convention that $0 \cdot [R : P_l] = 0$ even if $[R : P_l] = \infty$.)

Definition. *If $n = \sum_{l=0}^{\infty} \varepsilon_l(n)[R : P_l]$, where $0 \le \varepsilon_l(n) < [P_l : P_{l+1}]$, we call $\varepsilon_l(n)$ the l-th digit of n in the v-ary number system. Addition of numbers in v-ary arithmetic is performed by addition with carry on the vectors of digits, where a carry from position l to position $l+1$ occurs when the l-th digit reaches or exceeds $[P_l : P_{l+1}]$.*

If $[R_v : M_v]$ is finite, then $[P_l : P_{l+1}]$ divides $[{M_v}^l : {M_v}^{l+1}] = [R_v : M_v]$; if R_v/M_v is infinite, however, the digits need not be uniformly bounded or bounded at all. In the degenerate case, if N is maximal with $[R : P_N]$ finite, the N-th digit may be arbitrarily large, while for all $l > N$, $\varepsilon_l(n) = 0$ for all n.

If $n = \sum_{l=0}^{\infty} \varepsilon_l(n)[R : P_l]$, we set $r_j(n) = \sum_{l=0}^{j-1} \varepsilon_l(n)[R : P_l]$. This is consistent with our earlier use of $r_j(n)$ as the remainder of n under integral division by $[R : P_j]$, if $[R : P_j]$ is finite, and n otherwise.

Theorem 1. *Let $(a_i)_{i=0}^{n}$ be a v-sequence for R and for $0 \le k \le n$ let b_k be the binomial polynomial of degree k constructed from it. Then*

(a) $v\big(b_k(a_n)\big) = \big|\{l \ge 1 \mid r_l(k) > r_l(n)\}\big|$,

(b) $v\big(b_k(a_n)\big)$ *is the number of carries occurring in the addition of k and $n-k$ in v-ary arithmetic,*

(c) $v\big(b_k(a_n)\big) = 0 \quad \Longleftrightarrow \quad \forall\, l \;\; \varepsilon_l(k) \le \varepsilon_l(n)$ *in the v-ary number system.*

Proof. The condition $a_n \equiv a_i \bmod P_l$ with $0 \le i < r_l(k)$ is equivalent to $r_l(n) < r_l(k)$, such that (a) follows from Lemma 1. For all l, either $r_l(k) + r_l(n-k) = r_l(n)$, in which case no carry occurs at the l-th digit in the addition of k and $n-k$, or $r_l(k) + r_l(n-k) = [R : P_{l+1}] + r_l(n)$, in which case a carry does occur. In the first case, $r_l(k) \le r_l(n)$; in the second case, $r_l(k) > r_l(n)$ since $r_l(n-k) < [R : P_{l+1}]$. Thus (b) follows from (a). Since $\forall\, l\; \varepsilon_l(k) \le \varepsilon_l(n)$ is clearly the criterion for no carry to occur, (c) follows from (b). $\square$

Note that Theorem 1 (b) implies $v(b_k(a_n)) = v(b_{n-k}(a_n))$ for all $k \le n$.

In the case where $R = \mathbb{Z}$, $v = v_p$ and $a_n = n$, we retrieve Kummer's theorem that $v_p(\binom{n}{k})$ is equal to the number of $l \ge 1$ such that the remainder of k mod p^l is strictly greater than the remainder of n mod p^l, which number is also equal to the number of carries in the addition of k and $n-k$ in base p arithmetic [10; pp 115–119]. For an account of related facts about the classical binomial coefficients, see [17], for a different generalization, [9]. There is another version of Kummer's theorem that also carries over to generalized binomial coefficients in some cases.

Variant of Kummer's Theorem. *Let p be a prime, and $0 \le k \le n$. Then*

$$v_p\left(\binom{n}{k}\right) = \frac{1}{p-1}\sum_{l\ge 0} \varepsilon_l(k) + \varepsilon_l(n-k) - \varepsilon_l(n),$$

where $\varepsilon_l(j)$ means the l-th digit of j in base p.

We look at falling factorials: If $(a_i)_{i=0}^N$ is a v-sequence and $\alpha_i = a_N - a_{N-i}$, $i = 0,\ldots,N$, then $(\alpha_i)_{i=0}^N$ is a v-sequence with $\alpha_0 = 0$, and therefore homogeneous. Let $(\alpha_i)_{i=0}^N$ be a homogeneous v-sequence and $n \le N$, then $\alpha_1\ldots\alpha_n$ is a v-analogue of $n!$, since, for $n = \sum_{l=0}^m \varepsilon_l(n)[R:P_l]$

$$v(\alpha_1\ldots\alpha_n) \;=\; \sum_{j=1}^{m}\left[\frac{n}{[R:P_j]}\right] \;=\; \sum_{j=1}^{m}\sum_{l=j}^{m}\varepsilon_l(n)[P_j:P_l] \;=\; \sum_{l=1}^{m}\varepsilon_l(n)\sum_{j=1}^{l}[P_j:P_l].$$

If $[P_j:P_{j+1}] = q$ for all j (for instance, if R_v is the localization of R at a maximal ideal of finite index) this further simplifies to

$$\sum_{l=1}^{m}\varepsilon_l(n)\frac{(q^l-1)}{q-1} \;=\; \frac{1}{q-1}\left(\sum_{l=1}^{m}\varepsilon_l(n)q^l - \sum_{l=1}^{m}\varepsilon_l(n)\right) \;=\; \frac{1}{q-1}\left(n - \sum_{l=0}^{m}\varepsilon_l(n)\right),$$

and we can generalize the above variant of Kummer's theorem:

Theorem 2. *Let $(a_i)_{i=0}^n$ be a v-sequence for R and for $0 \le k \le n$ let b_k be the binomial polynomial of degree k constructed from it. If $[P_l : P_{l+1}] = q$ for all $l \ge 0$ then*

$$v(b_k(a_n)) \;=\; \frac{1}{q-1}\sum_{l\ge 0}\varepsilon_l(k) + \varepsilon_l(n-k) - \varepsilon_l(n)\,,$$

where $\varepsilon_l(j)$ denotes the l-th digit of j in base q.

Proof. This follows from the preceding calculations, since $b_k(a_n) =$

$$= \frac{\prod_{i=0}^{n-1}(a_n - a_i)}{\prod_{i=0}^{k-1}(a_k - a_i)\,\prod_{i=k}^{n-1}(a_n - a_i)} = \frac{\prod_{i=1}^{n}(a_n - a_{n-i})}{\prod_{i=1}^{k}(a_k - a_{k-i})\,\prod_{i=1}^{n-k}(a_n - a_{n-i})},$$

and $\alpha_i = a_n - a_{n-i}$ $(0 \le i \le n)$, $\beta_i = a_k - a_{k-i}$ $(0 \le i \le k)$ and $\gamma_i = a_n - a_{n-i}$ $(0 \le i \le n-k)$ are v-sequences, and homogeneous ones, since $\alpha_0 = \beta_0 = \gamma_0 = 0$. $\square$

4. Enumerating R Bijectively as an $\mathcal{I}$-Sequence. It is often possible to arrange all of R bijectively as a v-sequence. This has applications to interpolation by integer-valued polynomials.

Theorem 3. *If R is a countably infinite ring and $\mathcal{I} = \{I_n \mid n \in \mathbb{N}\}$ a descending chain of ideals of finite index in R with $\bigcap_{n\in\mathbb{N}} I_n = (0)$ then there exists an $\mathcal{I}$-sequence which enumerates R bijectively.*

Proof. Consider the elements of R labeled by natural numbers. (Such a label will be called the "number" of an element, not to be confused with the index at which it occurs in the sequence.) As the first step of constructing our sequence, we put $a_0 = 0$ and assign the different residue classes of I_1 other than I_1 itself to the indices $i = 1, \dots, [R : I_1] - 1$ in any order. We then define a_i to be the element with the smallest number in the residue class of I_1 assigned to i.

Assuming $a_0, \dots, a_{[R:I_{n-1}]-1}$ already defined, we define $a_{[R:I_{n-1}]}, \dots, a_{[R:I_n]-1}$ as follows. For $0 \leq i \leq [R : I_{n-1}] - 1$, assign the residue classes of I_n contained in $a_i + I_{n-1}$ but different from $a_i + I_n$ to the $[I_{n-1} : I_n] - 1$ indices $i + j[R : I_{n-1}]$ with $0 < j \leq [I_{n-1} : I_n] - 1$; then for $k = [R : I_{n-1}], \dots, [R : I_n] - 1$, define a_k to be the element with the smallest number in the residue class of I_n assigned to index k.

This procedure inductively defines an $\mathcal{I}$-sequence with the property that every sequence element a_i with $i < [R : I_n]$ is the element of lowest number in its residue class mod I_n. Since every $[R : I_n]$ consecutive sequence elements form a complete set of representatives mod I_n, every element of smallest number in its residue class mod I_n occurs among $a_0, \dots, a_{[R:I_n]-1}$.

$\bigcap_{I\in\mathcal{I}} I = (0)$ together with R being infinite implies that every $\mathcal{I}$-sequence is injective. Given $r \in R$, we show that it appears in the sequence: Since $\bigcap_{n\in\mathbb{N}} I_n = (0)$, there exists $N \in \mathbb{N}$, such that r is not congruent mod I_N to any element of smaller number. r is therefore the element of smallest number in its residue class mod I_N, and will appear among the first $[R : I_N]$ sequence elements. $\square$

Theorem 3 implies that every countably infinite subring R of a discrete valuation ring R_v can be arranged as a v-sequence, on condition that all intersections of powers of M_v with R are of finite index in R. For the application to interpolation, we use the fact that every function from the set $A = \{a_i \mid i \geq 0\}$ enumerated by a v-sequence $(a_i)_{i=0}^{\infty}$ to R_v can be represented as an infinite R_v-linear combination of the binomial polynomials b_n constructed from the sequence. (This infinite linear combination reduces to a finite sum upon evaluation at a_i, since $b_n(a_i) = 0$ for all $n > i$.)

Fact 2. *Let R be an infinite subring of a discrete valuation ring R_v, $(a_i)_{i=0}^{\infty}$ a v-sequence for R, $A = \{a_i \mid i \geq 0\}$ and*

$$b_0 = 1 \qquad \text{and} \qquad b_n(x) = \frac{\prod_{i=0}^{n-1}(x - a_i)}{\prod_{i=0}^{n-1}(a_n - a_i)} \qquad \text{for } n > 0$$

the binomial polynomials constructed from the sequence. Then every function $f : A \to R_v$ has a unique representation $f(x) = \sum_{i=0}^{\infty} d_i b_i(x)$ with $d_i \in R_v$.

Proof. From Lemma 1 we know that the b_n are in $\mathrm{Int}(R, R_v)$. By the definition of the binomial polynomials, $b_n(a_n) = 1$ and $b_n(a_i) = 0$ for $n > i$.

Every infinite R_v-linear combination of the b_i, $f = \sum_{i=0}^{\infty} d_i b_i$, represents a function $f\colon A \to R_v$, since it reduces to the finite sum $f(a_n) = d_n + \sum_{i=0}^{n-1} d_i b_i(a_n)$ upon evaluation at a_n and the b_i are in $\mathrm{Int}(R, R_v)$.

Conversely, given a function $f\colon A \to R_v$, we can define coefficients $d_i \in R_v$ inductively by $d_0 = f(a_0)$ and $d_n = f(a_n) - \sum_{i=0}^{n-1} d_i b_i(a_n)$, and find that $\sum_{i=0}^{\infty} d_i b_i$ represents the function f. $\square$

We can now give a short proof of the possibility of interpolation by integer-valued polynomials on a discrete valuation ring. (A more involved proof, which, however, has the advantage of determining, for each set of arguments in R, the minimal d such that there exists an interpolating polynomial of degree at most d for every choice of values in R_v, will appear in [5].)

Corollary to Theorem 3. *Let R be a countably infinite subring of a discrete valuation ring R_v with the property that for all n, $P_n = M_v^n \cap R$ is of finite index in R. Then for all $r_1, \ldots, r_m$ (distinct) in R and all $s_1, \ldots, s_m \in R_v$ there exists $f \in \mathrm{Int}(R, R_v)$ with $f(r_j) = s_j$ for $1 \le j \le m$.*

Proof. By the Krull Intersection Theorem, $\bigcap_{k=0}^{\infty} P_k = (0)$. Therefore there exists $n \in \mathbb{N}$ such that $r_1, \ldots, r_m$ are pairwise incongruent mod P_n. We show that $r_1, \ldots, r_m$ can be embedded in a v-sequence as elements of index $< [R{:}P_n]$. In the proof of Theorem 3, choose the initial numbering of the elements of R in such a way that r_j is element number j; each r_j is then the element of smallest number in its residue class mod P_n and will therefore occur among the first $N = [R : P_n]$ elements of the v-sequence $(a_i)_{i=0}^{\infty}$ so constructed. Now let b_k be the binomial polynomial of degree k constructed from $(a_i)_{i=0}^{\infty}$. Let $A = \{a_i \mid i \ge 0\}$. If we consider any function $\varphi\colon A \to R_v$ satisfying $\varphi(r_j) = s_j$ for $1 \le j \le m$, it has a representation as $\sum_{i=0}^{\infty} d_i b_i$ with $d_i \in R_v$ by Fact 2. Since $b_k(a_i) = 0$ for $k > i$, the values $\varphi(a_i)$ for $i < N$, and in particular $\varphi(r_j)$ for $1 \le j \le m$, are determined by $d_0, \ldots, d_{N-1}$. Therefore we can set $f = \sum_{i=0}^{N-1} d_i b_i$ and still have $f(r_j) = s_j$ for $1 \le j \le m$. As an R_v-linear combination of the $b_i \in \mathrm{Int}(R, R_v)$, f is in $\mathrm{Int}(R, R_v)$. $\square$

5. Explicit Construction for the Ring of Algebraic Integers in a Number Field. In some cases there is an explicit and natural bijective arrangement of R as a v-sequence, for instance, when R is the ring of algebraic integers in a number field K, $p \in \mathbb{Z}$ a prime such that only one prime ideal P of R lies above p, and R_v is the localization R_P of R at P. Since the intersections of the powers of the valuation ideal with R are just the powers of P, we need to construct an $\mathcal{I}$-sequence for $\mathcal{I} = \{P^n \mid n \in \mathbb{N}\}$ that enumerates R bijectively. We first show the existence of an integral basis of R having special properties with respect to a prime p. (For definitions of the notions related to the splitting of primes in number fields see [11]).

If $pR = P^e$ with $[R : P] = p^f$ and $\omega_1, \ldots, \omega_n$ is a $\mathbb{Z}$-basis of R, then

$$R = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n \quad \text{and} \quad P^e = pR = p\mathbb{Z}\omega_1 + \ldots + p\mathbb{Z}\omega_n,$$

but whether an element of R belongs to P^k for $0 < k < n$ is not readily seen from the coefficients in its representation as a $\mathbb{Z}$-linear combination of the ω_i. There are, however,

$\mathbb{Z}$-bases of R with the property that

$$P^k = p\mathbb{Z}\omega_1 + \ldots + p\mathbb{Z}\omega_{kf} + \mathbb{Z}\omega_{kf+1} + \ldots + \mathbb{Z}\omega_n.$$

More generally, we will show in Lemma 2 that if $pR = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$, and f_i denotes the inertial degree of $P_i \mid p$, there is a $\mathbb{Z}$-basis of R such that for $1 \le i \le r$ and $0 \le k \le e_i$,

$$\begin{aligned} P_i^k = \mathbb{Z}\omega_1^{(1)} + \ldots + \mathbb{Z}\omega_{e_1 f_1}^{(1)} + \ldots \\ + p\mathbb{Z}\omega_1^{(i)} + \ldots + p\mathbb{Z}\omega_{kf_i}^{(i)} + \mathbb{Z}\omega_{kf_i+1}^{(i)} + \ldots + \mathbb{Z}\omega_{e_i f_i}^{(i)} + \ldots \\ + \mathbb{Z}\omega_1^{(r)} + \ldots + \mathbb{Z}\omega_{e_r f_r}^{(r)}. \end{aligned}$$

Lemma 2. *Let K be an algebraic number field with $[K:\mathbb{Q}] = n$, R the ring of algebraic integers in K, and $p \in \mathbb{Z}$ a prime that splits in R as $pR = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ with $[R:P_i] = p^{f_i}$. Then there exists a $\mathbb{Z}$-basis of R consisting of blocks $\omega_1^{(i)}, \ldots, \omega_{e_i f_i}^{(i)}$, $1 \le i \le r$, such that for all $s \in R$, where*

$$s = m_1^{(1)}\omega_1^{(1)} + \ldots + m_{e_1 f_1}^{(1)}\omega_{e_1 f_1}^{(1)} + \ldots\ldots + m_1^{(r)}\omega_1^{(r)} + \ldots + m_{e_r f_r}^{(r)}\omega_{e_r f_r}^{(r)}$$

with $m_j^{(i)} \in \mathbb{Z}$, we have, for $1 \le i \le r$ and $1 \le k \le e_i$,

$$s \in P_i^k \quad \Longleftrightarrow \quad p \mid m_j^{(i)} \text{ for } 1 \le j \le kf_i\,.$$

Proof. For $1 \le i \le r$, let $V^{(i)} = R/P_i^{e_i}$ and $V = V^{(1)} \times \ldots \times V^{(r)}$. Also let $\pi: R \to R/pR$ be the canonical projection, $\varphi: R/pR \to V$ the isomorphism of rings $\varphi(s + pR) = (s + P_1^{e_1}, \ldots, s + P_r^{e_r})$, and $\rho_i: V \to V^{(i)}$ the projection of V onto the direct factor $V^{(i)}$. Then the composition $\rho_i\varphi\pi$ equals the canonical projection $\pi_i: R \to R/P_i^{e_i}$, $\pi_i(s) = s + P_i^{e_i}$.

$$\begin{array}{ccccccc} R & \xrightarrow{\pi} & R/pR & \xrightarrow{\varphi} & R/P_1^{e_1} \times \ldots \times R/P_r^{e_r} & \xrightarrow{\rho_i} & R/P_i^{e_i} \\ s & \longmapsto & s + pR & \longmapsto & (s + P_1^{e_1}, \ldots, s + P_r^{e_r}) & \longmapsto & s + P_i^{e_i} \end{array}$$

In $V^{(i)}$ the images $\pi_i(P_i^k) = V_k^{(i)}$, for $0 \le k \le e_i$, form a chain of ideals with $V_0^{(i)} = V^{(i)}$, $V_{e_i}^{(i)} = (0)$ and $[V_k^{(i)} : V_{k+1}^{(i)}] = p^{f_i}$. If we consider them as a chain of subspaces of the $\mathbb{Z}/p\mathbb{Z}$ vector space $V^{(i)}$, then $\dim(V_k^{(i)}) = (e_i - k)f_i$. By repeated basis completion, we get a $\mathbb{Z}/p\mathbb{Z}$-basis for $V^{(i)}$ with the property that for $k = 0, \ldots, e_i$ the last $(e_i - k)f_i$ basis elements form a basis of $V_k^{(i)}$; so that $v \in V^{(i)}$ is in $V_k^{(i)}$ if and only if the first $k \cdot f_i$ coefficients are zero in the representation of v as a $\mathbb{Z}_p$-linear combination of the basis elements.

Through the canonical embeddings of the direct factors we get a basis B of the $\mathbb{Z}/p\mathbb{Z}$ vector space V that consists of r blocks, the i-th of which is a basis of $V^{(i)}$, and such that $v \in V$ is in $\rho_i^{-1}(V_k^{(i)})$ if and only if the first $k \cdot f_i$ coordinates in the i-th block are zero in the representation of v with respect to basis B.

For $0 \le k \le e_i$, an element $s \in R$ is in P_i^k if and only if $\varphi\pi(s) \in \rho_i^{-1}(V_k^{(i)})$. Also, every $\mathbb{Z}$-basis Ω of R maps to a $\mathbb{Z}/p\mathbb{Z}$-basis C of V under $\varphi\pi$, and the coordinates of $\varphi\pi(s)$ with respect to C are just the coordinates of s with respect to Ω reduced mod p.

Therefore, if we can find a $\mathbb{Z}$-basis of R that maps to B under $\varphi\pi$, it will have the desired property. Let Ω be any $\mathbb{Z}$-basis of R and C its image under $\varphi\pi$. We may assume that the determinant of the basis transformation $\bar{T}$ of V that maps C to B is 1. (If not, multiply an element of B by the appropriate unit in $\mathbb{Z}/p\mathbb{Z}$; this does not affect the subspaces spanned by the blocks of B.) Since reduction mod p is surjective $\mathrm{SL}(\mathbb{Z}, n) \to \mathrm{SL}(\mathbb{Z}/p\mathbb{Z}, n)$ (see remark below), we can lift this basis transformation to $T \in \mathrm{SL}(\mathbb{Z}, n)$, apply T to Ω and get a $\mathbb{Z}$-basis for R that maps to B under $\varphi\pi$, as desired. $\square$

Remark. The easiest way to see that reduction of matrix entries mod p is surjective $\mathrm{SL}(\mathbb{Z}, n) \to \mathrm{SL}(\mathbb{Z}/p\mathbb{Z}, n)$ (I thank Paul Gerardin for pointing this out), is to observe that every matrix in $\mathrm{SL}(\mathbb{Z}/p\mathbb{Z}, n)$ is a product of elementary matrices (i.e., matrices with only 1s in the diagonal and only one non-zero off-diagonal entry) which can be lifted individually to elementary matrices over $\mathbb{Z}$ whose product is the desired lifting to $\mathrm{SL}(\mathbb{Z}, n)$.

Theorem 4. *Let $[K : \mathbb{Q}] = n$, R the ring of integers in K, and $p \in \mathbb{Z}$ a prime with $pR = P^e$, $[R : P] = p^f$, $ef = n$. Let $\omega_0, \ldots, \omega_{n-1}$ be a $\mathbb{Z}$-basis of R with the property that*

$$P^k = p\mathbb{Z}\omega_0 + \ldots + p\mathbb{Z}\omega_{kf-1} + \mathbb{Z}\omega_{kf} + \ldots + \mathbb{Z}\omega_{n-1} \quad \text{for} \quad 0 \le k \le e.$$

For $0 \le m < p^n$, with $m = \sum_{j=0}^{n-1} m_j p^j$ $(0 \le m_j < p)$, define $\beta(m) = \sum_{j=0}^{n-1} m_j \omega_j$, and for $l \in \mathbb{N}_0$ with $l = \sum_{j \ge 0} l_j p^{nj}$ $(0 \le l_j < p^n)$ let $\alpha(l) = \sum_{j \ge 0} \beta(l_j)(-p)^j$. Then

(a) $\qquad \alpha : \mathbb{N}_0 \to R$ *is bijective,*

(b) $\qquad \alpha(l) \in P^N \iff [R : P^N] \mid l,$

(c) $\qquad \alpha(l) - \alpha(l') \in P^N \iff [R : P^N] \mid l - l'.$

Proof. First note that for $0 \le k \le e$ we have $\beta(m) \in P^k$ if and only if $m_j = 0$ for $0 \le j < kf$, that is if and only if p^{kf} divides m. Also for $0 \le k \le e$, $\beta(m) - \beta(m') \in P^k$ if and only if $m_j = m'_j$ for $0 \le j < kf$, that is if and only if $m \equiv m' \bmod p^{kf}$.

Ad (b). $\alpha(l) \in P^N$, where $N = ke + r$ with $0 \le r < e$, if and only if $\beta(l_j) = 0$ for $j < k$ and $\beta(l_k) \in P^r$, that is if and only if $l_j = 0$ for $j < k$ and p^{rf} divides l_k, or equivalently, p^{kn+rf} divides l. Since $ef = n$, and therefore $p^{kn+rf} = p^{f(ke+r)} = [R : P^{ke+r}] = [R : P^N]$, we are done.

Ad (c). Similarly, $\alpha(l) - \alpha(l') \in P^{ke+r}$ if and only if $\beta(l) = \beta(l')$ for $j < k$ and $\beta(l_k) \equiv \beta(l'_k) \bmod P^r$. This is equivalent to $l_j = l'_j$ for $j < l$ and $l_k \equiv l'_k \bmod p^{rf}$, which is the case if and only if $l \equiv l' \bmod p^{kn+rf} = [R : P^{ke+r}]$.

Ad (a). Being a P-sequence, α is injective. To show surjectivity, we use the fact that every $m \in \mathbb{Z}$ has a representation $m = \sum_{j \ge 0} m_j (-p)^j$ with $0 \le m_j < p$, only finitely many $m_j \ne 0$. Given $a \in R$, $a = a_0\omega_0 + \ldots + a_{n-1}\omega_{n-1}$, with $a_k \in \mathbb{Z}$, $a_k = \sum_{j \ge 0} a_j^{(k)} (-p)^j$, $0 \le a_j^{(k)} < p$, let $l = \sum_{j \ge 0} \left(\sum_{k=0}^{n-1} a_j^{(k)} p^k \right) p^{nj}$, then $l_j = \sum a_j^{(k)} p^k$ for

$j \geq 0$, so $\beta(l_j) = \sum_{k=0}^{n-1} a_j^{(k)} \omega_k$, and $\alpha(l) = \sum_{j\geq 0} \beta(l_j)(-p)^j = \sum_{j\geq 0} \sum_{k=0}^{n-1} a_j^{(k)} \omega_k (-p)^j = \sum_{k=0}^{n-1} \big(\sum_{j\geq 0} a_j^{(k)} (-p)^j\big) \omega_k = a$. $\square$

REFERENCES

1. P.-J. Cahen, "Integer-valued polynomials on a subset," *Proc. Amer. Math. Soc.* **117** (1993), 919–929.
2. P.-J. Cahen, "Polynômes à valeurs entières," *Canad. J. Math.* **24** (1972), 747–754.
3. J.-L. Chabert, "Le groupe de Picard de l'anneau des polynômes à valeurs entières," *J. Algebra* **150** (1992), 213–230.
4. S. Frisch, "Integer-valued polynomials on Krull Rings," *Proc. Amer. Math. Soc.* **124** (12) (1996) 3595-3604.
5. S. Frisch, "Interpolation by integer-valued polynomials," to appear in J. Algebra.
6. R. Gilmer, W. Heinzer and D. Lantz, "The Noetherian property in rings of integer-valued polynomials," *Trans. Amer. Math. Soc.* **338** (1993), 187–199.
7. H. Gunji and D. L. McQuillan, "On a class of ideals in an algebraic number field," *J. Number Theory* **2** (1970), 207–222.
8. D. E. Knuth, *"The Art of Computer Programming" (second edition) vol. 2: "Seminumerical Algorithms,"* Addison-Wesley, Reading, MA, 1981.
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. E. Kummer, "Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen," *J. reine angew. Math.* **44** (1852), 93–146.
11. D. A. Marcus, *"Number Fields,"* Springer, New York, 1977.
12. H. Matsumura, *"Commutative ring theory,"* Cambridge University Press, 1986.
13. D. L. McQuillan, "On Prüfer domains of polynomials," *J. reine angew. Math.* **358** (1985), 162–178.
14. D. L. McQuillan, "Split primes and integer-valued polynomials," *J. Number Theory* **43** (1993), 216–219.
15. A. Ostrowski, "Über ganzwertige Polynome in algebraischen Zahlkörpern," *J. reine angew. Math.* **149** (1919), 117–124.
16. G. Pólya, "Über ganzwertige Polynome in algebraischen Zahlkörpern," *J. reine angew. Math.* **149** (1919), 97–116.
17. D. Singmaster, "Notes on binomial coefficients I–III," *J. London Math. Soc. (2)* **8** (1974), 545–560.

AMS 1991 Mathematics Subject Classification: 11B65, 05A10, 13G05.

Institut für Mathematik C
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
e-mail: frisch@blah.math.tu-graz.ac.at