When Does $\mathbf{m - n}$ Divide $\mathbf{f(m) - f(n)}$?

A Look at Column-Finite Matrices

DAVID CALLAN

Department of Statistics

University of Wisconsin-Madison

1210 W. Dayton St

Madison, WI 53706-1693

callan@stat.wisc.edu

In this paper, we consider the $\mathbf{Z}$-module of integer-valued functions f defined on the nonnegative integers (respectively on all integers), and characterize the submodule determined by the divisibility relation of the title, and also, as a corollary, by the divisibility relation $m+n|f(m)+f(n)$. Our results suggest some rather basic questions about such modules (equivalently, about infinite matrices of integers in which each column has only finitely many nonzero entries). We discuss these questions and pose a conjecture.

The functions f from the nonnegative integers $\mathbf{N}$ to the integers $\mathbf{Z}$ satisfying

$$m - n \mid f(m) - f(n) \qquad \textit{all } m, n \in \operatorname{dom} f \tag{1}$$

are mentioned in Apostol's textbook [1]. A Monthly problem [2] observes that integer-coefficient polynomials f certainly satisfy (1) and asks for a *nonpolynomial* function from $\mathbf{Z}$ to $\mathbf{Z}$ that does so. Problem 4 on the 1995 U.S.A. Mathematical Olympiad asks one to show that nonpolynomial functions from $\mathbf{N}$ to $\mathbf{Z}$ satisfying (1) never exhibit polynomial growth [3]. For sharper results on their growth, including an open question, see [4].

Our main result is that in both cases, $\mathbf{N}$ to $\mathbf{Z}$ and $\mathbf{Z}$ to $\mathbf{Z}$, there is a simple characterization of *all* functions satisfying (1); in fact in each case these functions form a $\mathbf{Z}$-module for which we can give a "basis". (In the present context the term basis, defined below, has the usual connotations of linearly spanning and being linearly independent, but infinite linear combinations are allowed.)

Let $M_{\mathbf{N}}$ (resp. $M_{\mathbf{Z}}$) denote the $\mathbf{Z}$-module of functions $\mathbf{N}$ to $\mathbf{Z}$ (resp. $\mathbf{Z}$ to $\mathbf{Z}$). Let M be any submodule of $M_{\mathbf{N}}$ or $M_{\mathbf{Z}}$ and let us define a *basis* for M as a finite or countably infinite set $\{f_0, f_1, f_2, \ldots\}$ in M for which each $f \in M$ has a unique expression (up to order of summands) as an integral linear combination $f = \sum_{k\geq 0} c_k f_k$. Naturally $(\sum_{k=0}^{\infty} c_k f_k)(n)$ means $\sum_{k=0}^{\infty} c_k f_k(n)$ and, to converge, the series must have only finitely many nonzero terms for any specific value of n (and hence of course order of summation does not matter). Equivalently, we may identify $f \in M_{\mathbf{N}}$ with the infinite sequence (row vector) $(f(j))_{j\geq 0}$, identify $M_{\mathbf{N}}$ with the set of all infinite sequences of integers, and view $\{f_i\}$ as an infinite matrix F with row i the sequence for f_i. Then $\sum_{k\geq 0} c_k f_k$ is the vector-matrix product $\mathbf{c}F$ and F must be column-finite (that is, only finitely many nonzero entries in each column) to ensure $\mathbf{c}F$ is defined for arbitrary $\mathbf{c}$. The conditions for $\{f_i\}$ to be a basis translate into: the rows of F (i) span $M_{\mathbf{N}}$, and (ii) are linearly independent (both conditions over $\mathbf{Z}$ and in the sense of infinite linear combinations). For example, the identity matrix corresponds to the "natural" basis $\{e_i\}_{i\geq 0}$ for $M_{\mathbf{N}}$ with $e_i(j) = \delta_{ij}$ (Kronecker delta). Pascal's matrix, given by $P = (\binom{j}{i})_{i,j\geq 0}$, corresponds to the basis $C_{\mathbf{N}} := \{f_i\}_{i\geq 0}$ with $f_i(j) = \binom{j}{i}$. The f_i form a basis because in fact $f = \sum_{i\geq 0} c_i f_i$ if and only if $c_j = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} f(i),\ j \geq 0$.

We digress to give one reason why $C_{\mathbf{N}}$ is a good basis to work with. Note $f_k(x) = \binom{x}{k}$ is a *polynomial* in x of degree k with rational coefficients; thus any *finite* integral linear combination of the f_k is a polynomial in the polynomial ring $\mathbf{Q}[x]$ that assumes integral values at the integers. Conversely, suppose $f(x) \in \mathbf{Q}[x]$ has this property. Let $\deg f = m$. Now $\{1, x, \ldots, x^m\}$ is a basis for the $\mathbf{Q}$-vector space $P_m = \{g(x) \in \mathbf{Q}[x] : \deg g \leq m\}$, and since $\deg f_k = k$, the set $\{f_k\}_{0\leq k\leq m}$ is also a basis for P_m. Hence $f = \sum_{k=0}^{m} c_k f_k$ with $c_k \in \mathbf{Q}$. In fact $c_k \in \mathbf{Z}$ by the integrality property of f and the last sentence of the preceding paragraph. It follows that the polynomial functions in $M_{\mathbf{N}}$ are precisely the finite integral linear combinations of the f_i. (It also follows that if $f \in \mathbf{Q}[x]$ assumes integral values at the nonnegative integers, then f assumes integral values at all integers, and hence the polynomial functions in $M_{\mathbf{Z}}$ are the same as the polynomial functions in $M_{\mathbf{N}}$.)

An analogous basis for $M_{\mathbf{Z}}$ is $C_{\mathbf{Z}} := \{g_k\}_{k\geq 0} \cup \{h_k\}_{k\geq 1}$ where $g_k(n) = \binom{n+k}{2k}$ and $h_k(n) = \binom{n+k-1}{2k-1}$. In this case, $f \in M_{\mathbf{Z}}$ can be (uniquely) expressed as $\sum_{k=0}^{\infty} c_k g_k + \sum_{k=1}^{\infty} d_k h_k$ with $c_n = \sum_{k=-n}^{n} (-1)^{n-k} \binom{2n}{n-k} f(k)$ for $n \geq 0$ and $d_n = \sum_{k=-n}^{n-1} (-1)^{n-k-1} \binom{2n-1}{n-k-1} f(k)$ for $n \geq 1$. By arranging $C_{\mathbf{Z}}$ in the order $g_0, h_1, g_1, h_2, g_2, \ldots$, and evaluating at the integers in the order $0, -1, 1, -2, 2, \ldots$, verification becomes equivalent to showing that the upper triangular matrices $(\binom{\lfloor i/2 \rfloor + (-1)^j \lceil j/2 \rceil}{i})_{i,j\geq 0}$ and $((-1)^{\lceil i/2 \rceil + \lfloor j/2 \rfloor} \binom{j}{\lceil (i+j)/2 \rceil})_{i,j\geq 0}$ are inverses of one another. This doesn't particularly facilitate a proof by hand (and we leave the combinatorial identities on which a formal proof rests to the interested reader), but a few minutes checking finite sections by computer will convince you these two matrices are indeed inverse to one another.

Note that h_k is an odd function, that is, $h_k(-n) = -h_k(n)$, $n \in \mathbf{Z}$, and for $k \geq 1$, $2g_k - h_k$ is an even function, as is g_0. Also, from the above formulas for c_n and d_n, if $f \in M_{\mathbf{Z}}$ is odd, it follows $c_k = 0$ for $k \geq 0$, and thus the h_k span the *odd* functions in $M_{\mathbf{Z}}$. Similarly if $f \in M_{\mathbf{Z}}$ is even, $c_k = -2d_k$ for $k \geq 1$, yielding a spanning set for the even functions.

Summarizing, we have the following theorem.

Theorem 1 *Let* $f_k(n) = \binom{n}{k}$, $g_k(n) = \binom{n+k}{2k}$, $h_k(n) = \binom{n+k-1}{2k-1}$ *as above.*

Then

(i) $C_{\mathbf{N}} = \{f_k\}_{k\geq 0}$ *is a basis for* $M_{\mathbf{N}}$.

(ii) $C_{\mathbf{Z}} = \{g_k\}_{k\geq 0} \cup \{h_k\}_{k\geq 1}$ *is a basis for* $M_{\mathbf{Z}}$.

(iii) $C_{\text{odd}} = \{h_k\}_{k\geq 1}$ *is a basis for* $\{f \in M_{\mathbf{Z}} : f \text{ is odd}\}$;

. $C_{\text{even}} = \{g_0\} \cup \{2g_k - h_k\}_{k\geq 1}$ *is a basis for* $\{f \in M_{\mathbf{Z}} : f \text{ is even }\}$.

Just as for $C_{\mathbf{N}}$, the finite integral linear combinations in $C_{\mathbf{Z}}, C_{\text{odd}}, C_{\text{even}}$ comprise the polynomial functions in the respective modules. The latter facts—at least for $C_{\mathbf{N}}, C_{\text{odd}}, C_{\text{even}}$—are noted in Pólya and Szegö [5].

For the sake of clarity, we mostly use the function interpretation for $M_{\mathbf{N}}$ and $M_{\mathbf{Z}}$ in the first part of the paper—Theorems 1 through 4—and then work with sequences and matrices in the second part. We are now ready to state our main result. Let $\text{lcm}[n]$ denote the least common multiple of the first n positive integers (and set $\text{lcm}[0] = 1$).

Theorem 2 *Let $M'_{\mathbf{N}}$ (resp. $M'_{\mathbf{Z}}$) denote the submodule of functions f in $M_{\mathbf{N}}$ (resp. $M_{\mathbf{Z}}$) that satisfy* (1) : $m-n|f(m)-f(n)$ *for all* $m,n\in \operatorname{dom} f$.

Then

(i) $M'_{\mathbf{N}}$ *has a basis* $C'_{\mathbf{N}}=\{\mathrm{lcm}[k]f_k\}_{k\geq 0}$.

(ii) $M'_{\mathbf{Z}}$ *has a basis* $C'_{\mathbf{Z}}=\{\mathrm{lcm}[2k]g_k\}_{k\geq 0}\cup\{\mathrm{lcm}[2k-1]h_k\}_{k\geq 1}$.

Proof. First we develop a couple of lemmas. Let $[a,b]$ denote the interval of integers $a,a+1,\ldots,b$. For prime p and positive integer n, let $\nu_p(n)$ denote the exponent of the largest power of p that divides n; thus $p^{\nu_p(n)}|n$ but $p^{\nu_p(n)+1}\not| n$. It is trivial that $\lfloor\frac{a}{c}\rfloor+\lfloor\frac{b}{c}\rfloor\leq\lfloor\frac{a+b}{c}\rfloor$ for positive integers a,b,c. Hence for $n\geq k\geq 1$ and $r\geq 1$, $\lfloor k/p^r\rfloor\leq\lfloor n/p^r\rfloor-\lfloor(n-k)/p^r\rfloor$. This says that for each r the number of integers in $[1,k]$ divisible by p^r is $\leq$ the number in $[n-k+1,n]$ so divisible. This fact allows the construction in an obvious way of a bijection $\phi:[1,k]\to[n-k+1,n]$ such that $\nu_p(i)\leq\nu_p(\phi(i))$ for $1\leq i\leq k$. (Consider first the integers in $[1,k]$ divisible by the highest power of p that divides k. Let ϕ be any one-to-one map from these integers to the integers in $[n-k+1,n]$ divisible by this power of p and then proceed in turn to the smaller powers of p.) Let $n^{\underline{k}}$ denote the falling factorial $n(n-1)(n-2)\cdots$ to k factors.

Lemma 1 .

(i) For $n\geq k\geq 1$ and p prime, $p^{\nu_p(k!)}|n^{\underline{k}}$.

(ii) If i $(1\leq i<k)$ factors are removed from the product $n^{\underline{k}}$, then the resulting product is divisible by $p^{\nu_p(k!)-i\nu_p(\mathrm{lcm}[k])}$.

Proof. (i) Since $\binom{n}{k}=\frac{n^{\underline{k}}}{k!}$ is an integer, $p^{\nu_p(k!)}|n^{\underline{k}}$.

(ii) This assertion follows from part (i) and the existence of the bijection ϕ which says, so far as divisibility by p goes, the effect of tossing the factor $\phi(i)$ out of the product $n^{\underline{k}}$ is no worse than the effect of tossing the factor i out of $k!$, and $\nu_p(i)\leq\nu_p(\mathrm{lcm}[k])$.

We also need a result on divisibility of binomial coefficients.

Lemma 2 *If p is a prime which does not divide r, and if $i>j\geq 0$, then*

$$p^{i-j}|\binom{p^i q}{p^j r}.$$

Proof. An often-quoted result of Kummer (see [6] for a proof) says that the exact power of p that divides a binomial coefficient $\binom{n}{k}$ is the number of "borrows" when k is subtracted from n in base p. For example in base 5, $(375)_5 = 3000$, $(330)_5 = 2310$, and we have the subtraction

$$\begin{array}{rcllll} n & = & 3 & 0 & 0 & 0 \\ k & = & 2_1 & 3_1 & 1 & 0 \\ n-k & = & & 1 & 4 & 0 \end{array}$$

with 2 borrows. Note that if (as here) the number of trailing zeros in n exceeds that in k, the number of borrows will always be at least the excess (here, 2). Since $k = p^j r$ has exactly j trailing zeros, this observation translates immediately into Lemma 2.

Now to the proof of the theorem. First we must show the elements of $C'_{\mathbf{N}}$ actually satisfy (1). Thus let $f'_k(n) = \mathrm{lcm}[k]\binom{n}{k}$ denote a typical element of $C'_{\mathbf{N}}$ and we must show for $m, n, k \geq 1$, that $m | f'_k(n+m) - f'_k(n)$, that is, $m | \mathrm{lcm}[k]((n+m)^{\underline{k}} - n^{\underline{k}})/k!$ or, equivalently, for each prime divisor p of m

$$p^{\nu_p(m)+\nu_p(k!)-\nu_p(\mathrm{lcm}[k])} | (n+m)^{\underline{k}} - n^{\underline{k}} \tag{2}$$

If $\nu_p(m) \leq \nu_p(\mathrm{lcm}[k])$, (2) is an immediate consequence of Lemma 1(i). So suppose $\nu_p(m) > \nu_p(\mathrm{lcm}[k])$ and consider the cases $k > n$ and $k \leq n$ separately. If $k > n$, then m is one of the factors in $(n+m)^{\underline{k}}$ and $n^{\underline{k}} = 0$. But $p^{\nu_p(m)} | m$ by definition, and $p^{\nu_p(k!)-\nu_p(\mathrm{lcm}[k])} | \frac{(n+m)^{\underline{k}}}{m}$ by Lemma 1(ii), and (2) is obtained by multiplying these divisibility relations. On the other hand, if $k \leq n$ consider the powers of m in the expansion $(n+m)^{\underline{k}} - n^{\underline{k}} = \sum_{i=1}^{k} [\Sigma \pi(k-i)] m^i$, where, in the inner sum, the summand $\pi(k-i)$ runs over all products of $k-i$ factors from $[n-k+1, n]$. We have $p^{\nu_p(k!)-i\nu_p(\mathrm{lcm}[k])} | \pi(k-i)$ by Lemma 1(ii) and trivially $p^{\nu_p(m)i} | m^i$. This yields $p^{\nu_p(k!)+i(\nu_p(m)-\nu_p(\mathrm{lcm}[k]))} | \pi(k-i)m^i$ and hence certainly $p^{\nu_p(k!)+\nu_p(m)-\nu_p(\mathrm{lcm}[k])} | \pi(k-i)m^i$ since $i \geq 1$ and, by supposition, $\nu_p(m) > \nu_p(\mathrm{lcm}[k])$. Summing over i we obtain (2). Thus $C'_{\mathbf{N}} \subseteq M'_{\mathbf{N}}$, and the proof that $C'_{\mathbf{Z}} \subseteq M'_{\mathbf{Z}}$ is very similar.

Next we must show that every $f \in M'_{\mathbf{N}}$ is an integral linear combination of the elements of $C'_{\mathbf{N}}$. We already know there exists a unique sequence of integers $(c_n)_{n \geq 0}$ (namely, $c_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$) such that $f(n) = \sum_{k=0}^{n} c_k \binom{n}{k}$. So we must show that $\mathrm{lcm}[k] | c_k$ under the hypothesis that f satisfies (1). To get induction (on n) working, we'll prove a little more:

$$\textit{for all } a \in \mathbf{N},\ \mathrm{lcm}[n] \textit{ divides } c_n(a) := \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(a+k) \textit{ when } f \textit{ satisfies } (1)$$

(Of course, $c_n(0) = c_n$ and, to numerical analysts, $c_n(a)$ is the nth forward difference of f at a.) The base case $n = 1$ is trivial. Since $c_n(a) = c_{n-1}(a+1) - c_{n-1}(a)$ we have by the induction hypothesis that $\mathrm{lcm}[n-1] | c_n(a)$ and need only show $n | c_n(a)$. Let p be any prime divisor of n. Write $n = p^i r$ and let $k = p^j s$ with r, s relatively prime to p. Now (1) implies $p^j | f(a+k) - f(a)$. Also if $i \geq j$, then $p^{i-j} | \binom{n}{k}$ by Lemma 2. In any case, $p^i | \binom{n}{k} [f(a+k) - f(a)]$. Since $c_n(a) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} [f(a+k) - f(a)]$, it follows that $p^i | c_n(a)$ and since p is arbitrary, $n | c_n(a)$ and the induction is complete. The corresponding proof that $C'_{\mathbf{Z}}$ generates $M'_{\mathbf{Z}}$ is analogous: $c_n(a)$ and $d_n(a)$ are defined analogously (except now $a \in \mathbf{Z}$) and the induction is based on the recurrence relations $c_n(a) = d_n(a+1) - d_n(a)$ and $d_n(a) = c_{n-1}(a) - c_{n-1}(a-1)$. This completes the proof of Theorem 2.

Here's one corollary. As noted earlier, the finite linear combinations in $C_{\mathbf{N}}$ (or $C_{\mathbf{Z}}$) yield polynomials, and infinite linear combinations nonpolynomials (by uniqueness—the polynomials are already exhausted by the finite linear combinations). The observation (made in the editorial comment on [2]) that there are uncountably many nonpolynomial functions $\mathbf{Z}$ to $\mathbf{Z}$ satisfying (1) follows immediately.

For later use we remark that the divisibility relation (2) above in fact holds for arbitrary integer n. (This shows that $f'_k(n) = \mathrm{lcm}[k]\binom{n}{k}$, if considered as a function of $n \in \mathbf{Z}$ rather than just $n \in \mathbf{N}$, is in $M'_{\mathbf{Z}}$; thus each element of the basis $C'_{\mathbf{N}}$ for $M'_{\mathbf{N}}$ extends to an element of $M'_{\mathbf{Z}}$. We will soon see that not every element of $M'_{\mathbf{N}}$ extends in this fashion.) The proof of (2) for $n \leq 0$ is similar to that given above for $n \geq 1$: $n = 0$ is easy, so suppose $n < 0$. In case $n+m < 0$ the result already established in (2) for $n \geq 1$ applies (with the roles of $n+m$ and n reversed); the case $n + m \geq 0$ should be split into subcases $k > n+m$ and $k \leq n+m$ corresponding to the subcases $k > n$ and $k \leq n$ above. The details are left to the reader.

Now we consider an interesting submodule of $M'_{\mathbf{N}}$. Let $\theta : M_{\mathbf{Z}} \to M_{\mathbf{N}}$ be given by restriction of domain, that is, $\theta(f) = f_{|\mathbf{N}}$. (Interpreting the elements of $M_{\mathbf{N}}$ and $M_{\mathbf{Z}}$ as sequences, θ just throws away the left half of a doubly infinite sequence.) Let ψ denote the restriction of θ to

$M'_{\mathbf{Z}}$; then it is clear that $\psi : M'_{\mathbf{Z}} \to M'_{\mathbf{N}}$. Note that the range of ψ includes at least all the finite integral linear combinations of $C'_{\mathbf{N}}$, that is, all the polynomial maps in $M'_{\mathbf{N}}$. This is because each $f'_k \in C'_{\mathbf{N}}$ extends, as remarked in the previous paragraph, to an element in $M'_{\mathbf{Z}}$. Of course the map θ is onto but far from one-to-one. Contrariwise, we have the following result for ψ.

Theorem 3 *Let $\psi : M'_{\mathbf{Z}} \to M'_{\mathbf{N}}$ be the map just defined. Then*

(i) ψ is one-to-one.

(ii) ψ is not onto.

Proof. (i) It suffices to show $\ker \psi = (0)$ and to see this, view an element of $\ker \psi$ as a doubly infinite sequence of integers with a tail of zeros. Then it cannot have any nonzero term (the standing divisibility hypothesis (1) implies any term is divisible by all sufficiently large integers).

(ii) Recall $f_k(n) = \binom{n}{k}$ and for brevity set $u_k = \mathrm{lcm}[k],\ k \geq 0$. Now consider the element of $M'_{\mathbf{N}}$ given by $f = \sum_{k\geq 0} u_k f_k$ and let us ask if f can be extended backwards, i.e. defined at -1, to yield a (sequence of integers) g that is still in $M'_{\mathbf{N}}$. It suffices to show this cannot be done. Suppose it can. Then by Theorem 2(i), $g = \sum_{k\geq 0} c_k u_k f_k$ for some sequence of integers (c_k) and $g(n+1) = f(n),\ n \geq 0$. This readily implies that $u_k = c_k u_k + c_{k+1}u_{k+1},\ k \geq 0$. Multiply by $(-1)^k$ and add to obtain $\sum_{k=0}^{n-1}(-1)^k u_k = c_0 u_0 + (-1)^{n-1} c_n u_n$ and in particular,

$$\sum_{k=0}^{n} (-1)^k u_k \equiv c_0 \pmod{u_n} \qquad\qquad n \geq 1 \tag{3}$$

This infinite set of congruences has no solution for c_0 as follows. Let $s_n = \sum_{k=0}^{n}(-1)^k u_k$ denote the left side of (3). Since $u_n = u_{n-1}$ unless n is a prime power, p^r, in which case $u_n = pu_{n-1}$, it is easy to show by induction that $0 < s_n < u_n$ for n even ≥ 2, and $-u_n < s_n < 0$ for n odd ≥ 3. Thus if $c_0 \geq 0$ we have for all sufficiently large even n, $0 \leq c_0 < u_n$ while $0 < s_n < u_n$ and, by (3), $s_n \equiv c_0 \pmod{u_n}$, hence $s_n = c_0$. It follows that $s_{n+2} = s_n$ and so $u_{n+2} = u_{n+1}$, a contradiction since $u_{n+2} = 2u_{n+1}$ whenever $n+2$ is a power of 2. A similar contradiction is obtained in case $c_0 < 0$, completing the proof.

As a curiosity, we can now "analyze" the divisibility relation $m + n | f(m) + f(n)$ with little extra effort. Let $M''_{\mathbf{N}} = \{f \in M_{\mathbf{N}} : m+n | f(m) + f(n),\ m, n \in \mathbf{N}\}$ and analogously for $M''_{\mathbf{Z}}$.

Also let $\rho : M''_{\mathbf{Z}} \to M''_{\mathbf{N}}$ denote the restriction map analogous to $\psi : M'_{\mathbf{Z}} \to M'_{\mathbf{N}}$ above.

Theorem 4 *Let $h_k(n) = \binom{n+k-1}{2k-1}$ as in Theorem 1, and let $h_{k|\mathbf{N}}$ denote the restriction of h_k to* $\mathbf{N}$. *Then*

(i) $\{\mathrm{lcm}[2k-1]h_{k|\mathbf{N}}\}_{k\geq 1}$ *is a basis for* $M''_{\mathbf{N}}$.

(ii) $\{\mathrm{lcm}[2k-1]h_k\}_{k\geq 1}$ *is a basis for* $M''_{\mathbf{Z}}$.

(iii) $\rho : M''_{\mathbf{Z}} \to M''_{\mathbf{N}}$ *is both one-to-one and onto (unlike the map ψ of Theorem 3).*

Proof. Suppose $f \in M''_{\mathbf{Z}}$. The divisibility hypothesis with $m = -n$ implies f is odd, and consequently the divisibility hypothesis is equivalent to $m - n | f(m) - f(n),\ m, n \in \mathbf{Z}$. Hence $M''_{\mathbf{Z}} = M'_{\mathbf{Z}} \cap \{f \in M_{\mathbf{Z}} : f \text{ is odd}\}$ and part (ii) follows from Theorems 1(iii) and 2(ii). Now observe that $m + n | f(m) + f(n),\ m, n \in \mathbf{N}$ implies also $m - n | f(m) - f(n),\ m, n \in \mathbf{N}$, or equivalently, $k | f(\ell + k) - f(\ell),\ k, \ell \in \mathbf{N}$. To see this, write $\ell = kq + r$ with $0 \leq r < k$ (division algorithm) and apply the hypothesis with $m = kq + r$ and $n = k - r$ to obtain $k | f(kq + r) + f(k - r)$. Replacing q by $q + 1$ yields $k | f(kq + r + k) + f(k - r)$. Hence k divides the difference, that is, $k | f(\ell + k) - f(\ell)$, as desired.

This permits us to extend any $f \in M''_{\mathbf{N}}$ to $f \in M''_{\mathbf{Z}}$ by defining $f(-n) = -f(n),\ n \geq 1$, (the reader should check this) and this is the *only* way to extend f since $M''_{\mathbf{Z}}$ consists of odd functions. Thus the restriction map $\rho : M''_{\mathbf{Z}} \to M''_{\mathbf{N}}$ is one-to-one and onto. This is part (iii) and part (i) follows from parts (ii) and (iii).

The preceding results raise the question: to what extent is the above notion of "basis" analogous to a free basis (of a finitely generated module)? To begin with, any finitely generated submodule of $M_{\mathbf{N}}$ is a free $\mathbf{Z}$-module and here the notions "basis" as above and "free basis" coincide. Every submodule M of $M_{\mathbf{N}}$ does possess a basis. To see this, view elements of $M_{\mathbf{N}}$ as sequences, and for $i \geq 0$ let c_i denote the least positive integer occurring in position i among elements of M having zeros in the positions preceding i (but if all of these elements have 0 in position i, take $c_i = 0$). If $c_i \neq 0$ let $\mathbf{u}_i$ be any such sequence (with first nonzero entry c_i in position i). Then it is straightforward to verify that these $\mathbf{u}_i$ form a basis for M.

Now we switch perspective from functions and lists of functions to sequences and matrices, and henceforth write $\mathbf{Z}^\infty$ instead of $M_{\mathbf{N}}$ for the infinite sequences of integers (and $\mathbf{Q}^\infty$ for the infinite sequences of rationals). Also $\mathbf{Z}_\infty$ (resp. $\mathbf{Q}_\infty$) will be used to denote the set of infinite matrices of integers (resp. rationals). The terms "span" and "linear independence" will continue to be used in the sense of infinite linear combinations. For $A \in \mathbf{Z}_\infty$ let $R(A)$ denote the set of rows of A. One basic question is: When does $R(A)$ form a basis for $\mathbf{Z}^\infty$? First, as noted above, A must be column-finite. Second, for $R(A)$ to span $\mathbf{Z}^\infty$, it is certainly necessary for $R(A)$ to span the "basic" vectors $\{e_k\}$, equivalently, A must possess a left inverse in $\mathbf{Z}_\infty$, call it B. Third, A must have a trivial left nullspace in $\mathbf{Z}^\infty$ (so A's rows are linearly independent) and this makes A's left inverse B unique. These three conditions, though, do not ensure $R(A)$ spans all of $M_\mathbf{N}$.

Example 1 *Let J denote the infinite "Jordan" matrix—all 0's except 1's just below the main diagonal—and set $A = I + 2J$. Then A is column-finite and has a unique left inverse in $\mathbf{Z}_\infty$, but A's rows do not have $\mathbf{Z}$-span $\mathbf{Z}^\infty$.*

Proof. The column-finiteness of A is obvious. It is easy to check that J^k has 1's on the kth diagonal below and parallel to the main diagonal and 0's elsewhere, and that a left inverse of A in $\mathbf{Z}_\infty$ is given correctly by the formal expansion $(I+2J)^{-1} = I - 2J + 4J^2 - 8J^3 + \ldots$. The left nullspace of A in $\mathbf{Q}^\infty$ is spanned by $(1, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{8}, \ldots)$ and so clearly has trivial intersection with $\mathbf{Z}^\infty$, making A's left inverse in $\mathbf{Z}_\infty$ unique. On the other hand, let $\mathbf{e}$ denote the (row) vector of all 1's. Then $\mathbf{e}A = 3\mathbf{e}$, so the general solution of $\mathbf{x}A = \mathbf{e}$ in $\mathbf{Q}^\infty$ is $\mathbf{x} = \frac{1}{3}\mathbf{e} + k(1, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{8}, \ldots)$ (arbitrary $k \in \mathbf{Q}$) and clearly $\mathbf{x} \notin \mathbf{Z}^\infty$ for any k. Thus $\mathbf{e}$ is not in the $\mathbf{Z}$-row-span of A.

Column-finiteness of A's left inverse (or rather the lack of it) plays a role in the preceding example. Note that a product of column-finite matrices is again column-finite, and associativity holds: in fact for $\mathbf{w} \in \mathbf{Q}^\infty$ and $X, Y \in \mathbf{Q}_\infty$, if wX is defined and Y is column-finite, then it is easy to check all four products are defined and $(\mathbf{w}X)Y = \mathbf{w}(XY)$. Three corollaries: (1) If X, Y are column-finite matrices in $\mathbf{Q}_\infty$, then $(WX)Y = W(XY)$ for arbitrary $W \in \mathbf{Q}_\infty$. (2) The column-finite matrices in $\mathbf{Q}_\infty$ form a ring (with identity). Let us denote this ring by $\mathrm{CF}(\mathbf{Q}_\infty)$ (CF for column-finite) and analogously for $\mathrm{CF}(\mathbf{Z}_\infty)$. (3) If $A \in \mathrm{CF}(\mathbf{Z}_\infty)$ has a unique left inverse B in $\mathbf{Z}_\infty$ *that happens to be column-finite*, then we have for arbitrary $\mathbf{w} \in \mathbf{Z}^\infty$, $\mathbf{w} = \mathbf{w}(BA) = (\mathbf{w}B)A$ and thus $R(A)$ does indeed have $\mathbf{Z}$-span $\mathbf{Z}^\infty$. Of course this argument breaks down if B is not column-finite since then $\mathbf{w}B$ might not be defined (and Example 1 shows the conclusion need not hold). For $A \in \mathrm{CF}(\mathbf{Z}_\infty)$, the assertion that A has a unique left inverse in $\mathbf{Z}_\infty$ that happens to lie in $\mathrm{CF}(\mathbf{Z}_\infty)$ is, on the face of it, stronger than saying that A has a unique left inverse in $\mathrm{CF}(\mathbf{Z}_\infty)$. In fact the two statements are equivalent since if A has a left inverse B in $\mathrm{CF}(\mathbf{Z}_\infty)$ and another left inverse C in $\mathbf{Z}_\infty \backslash \mathrm{CF}(\mathbf{Z}_\infty)$, then $B - C$ has a nonzero row and adding this row to any row of B produces another left inverse for A in $\mathrm{CF}(\mathbf{Z}_\infty)$. Furthermore, from elementary ring theory, for a in any ring with identity R, "a has a unique left inverse in R" is equivalent to "a is invertible (i.e. a unit) in R".

These observations suggest the following conjecture.

Conjecture Let A be a column-finite infinite matrix of integers, that is, $A \in \mathrm{CF}(\mathbf{Z}_\infty)$.

Then the rows of A form a basis for $\mathbf{Z}^\infty$ if and only if A is a unit in $\mathrm{CF}(\mathbf{Z}_\infty)$.

(We have proved the "if" part and for the "only if" part we've shown that A has a unique left inverse B in $\mathbf{Z}_\infty$. The conjecture then is that B must lie in $\mathrm{CF}(\mathbf{Z}_\infty)$.)

Motivated by the preceding observations, let us now consider the subtleties of the concept of inverse for an infinite matrix. In general, we must distinguish between left and right inverses—indeed over the integers, all nine combinations of 0,1 or infinitely many left inverses and 0,1 or infinitely many right inverses are possible. The following table provides simple examples (J denotes the Jordan matrix with 1's below the diagonal, K is given below, ^{t} denotes transpose).

Example 2

		# right inverses		
		0	1	∞
#	0	O	K^t	J^t
left	1	K	I	$I + J^t$
inverses	∞	J	$I + J$	$J + J^t$

Here the unique left inverse of K and K itself are given respectively by

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & -1 & 1 & 0 & 0 & \\ 0 & -1 & 0 & 1 & 0 & \\ 0 & -1 & 0 & 0 & 1 & \\ 0 & -1 & 0 & 0 & 0 & \\ \vdots & & & & & \ddots \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots \\ 1 & 0 & 0 & 0 & 0 & \\ 1 & 1 & 0 & 0 & 0 & \\ 1 & 0 & 1 & 0 & 0 & \\ 1 & 0 & 0 & 1 & 0 & \\ \vdots & & & & & \ddots \end{pmatrix}$$

For $J + J^t$, a right inverse is $J - J^3 + J^5 - \dots$ (note $J^t J = I$), and a right nullvector is $(1, 0, -1, 0, 1, 0, -1, \dots)^t$. These and the other easy verifications are left to the reader.

We now collect a few simple facts about inverses of column-finite matrices.

Proposition 1 *If $A \in \mathrm{CF}(\mathbf{Z}_\infty)$ has a* unique *left inverse B in $\mathbf{Z}_\infty$ and if AB is defined, then $AB = I$.*

Proof. By associativity, $(AB - I)A = A(BA) - A = O$. Hence $AB - I = O$ by uniqueness of A's left inverse.

A diagonal matrix $D \in \mathbf{Q}_\infty$ with nonzero diagonal entries obviously has an unambiguous inverse $D^{-1} \in \mathbf{Q}_\infty$, but already with triangular matrices we must be careful.

Proposition 2 *Suppose $U \in \mathrm{CF}(\mathbf{Q}_\infty)$ is block upper triangular with finite square blocks $\{U_{ii}\}$ on the main diagonal.*

If the U_{ii} are invertible, then U has a unique left inverse V in $\mathbf{Q}_\infty$ and V is block upper triangular. Moreover, V is a right inverse for U and it is the only column-finite *right inverse for U in $\mathbf{Q}_\infty$, though U may have other right inverses in $\mathbf{Q}_\infty$ and even in $\mathbf{Z}_\infty$.*

Also, if U has integer entries and the U_{ii} are invertible over $\mathbf{Z}$, then V is actually in $\mathbf{Z}_\infty$.

Proof. We can solve $VU = I$ uniquely for the blocks of V in turn: first row, left to right, then second row, left to right, etc, and V has the stated form. In particular, V is column-finite; so UV is defined and by Prop. 1, $UV = I$.

Similarly, if W is assumed column-finite, we can solve $UW = I$ uniquely for the (block) columns of W left to right, bottom to top. Hence W must equal V. (Alternatively, invoke the result for rings: if $vu = 1$ and $uw = 1$, then $w = v$.) However for the upper triangular matrix $U = I + J^t$ with J the "Jordan" matrix above, $U(1, -1, 1, -1, 1, \ldots)^t = \mathbf{0}$ showing that U has multiple right inverses.

With U, V as in Prop. 2, uniqueness of U's right inverse may be guaranteed by U's zero pattern.

Proposition 3 *With U, V as in Prop. 2, suppose U satisfies the following condition:*

$$U\mathbf{x} \text{ is defined (i.e. involves no infinite sums) only when } \mathbf{x} \text{ is column-finite} \tag{4}$$

(e.g. (4) certainly holds if U's above-diagonal entries are all nonzero.)

Then V is the unique *right inverse for U in $\mathbf{Q}_\infty$.*

Proof. Suppose $U\mathbf{x} = \mathbf{0}$. By (4) there exists n such that $x_i = 0$ for $i > n$. Take a large enough square upper left submatrix U_m consisting of whole blocks of U so its size is m by m with $m \geq n$. Then $U_m(x_1, x_2, \ldots, x_m)^t = \mathbf{0}$ and since U_m is a finite invertible matrix, $\mathbf{x} = \mathbf{0}$ and U has trivial right nullspace, making any right inverse for U unique.

Proposition 4 *With U, V again as in Prop. 2, condition (4) of Prop. 3 is satisfied if and only if there exists $k \geq 1$ such that the submatrix of U consisting of its first k rows has only finitely many zero columns.*

Proof. Exercise.

Corollary Pascal's matrix of binomial coefficients, $P = (\binom{j}{i})_{i,j \geq 0}$, has a unique left inverse and a unique right inverse, and both are given by $P^{-1} = ((-1)^{j-i}\binom{j}{i})$.

Proof. One verifies that $Q = ((-1)^{j-i}\binom{j}{i})$ is a left inverse for P, unique by Prop. 2, hence $PQ = I$ by Prop. 1, and Q is P's unique right inverse by Prop. 3.

Referring back to Example 1, note the matrix A given there has multiple left inverses in $\mathbf{Q}_\infty$. This raises the question: does the phenomenon of Example 1 occur in $\mathbf{Q}_\infty$? Perhaps things are nicer over fields and for a matrix $A \in \mathrm{CF}(\mathbf{Q}_\infty)$ with a unique left inverse B in $\mathbf{Q}_\infty$, perhaps B must lie in $\mathrm{CF}(\mathbf{Q}_\infty)$.

Here are several other questions. Is there an effective method to determine which elements of $M'_{\mathbf{N}}$ are in the range of ψ? When can a subset of $M_{\mathbf{N}}$ $(= \mathbf{Z}^\infty)$ be enlarged to a basis? Could the matrix K of Example 2 be replaced by a column-finite matrix, that is, in view of Prop. 1, could a matrix $A \in \mathrm{CF}(\mathbf{Z}_\infty)$ have a unique left inverse B in $\mathbf{Z}_\infty$ for which AB is not defined? In the rings $\mathrm{CF}(\mathbf{Z}_\infty)$ and $\mathrm{CF}(\mathbf{Q}_\infty)$, is there a nice characterization (or generating set) for the units? An answer to the latter question for matrices A that are both row- and column-finite and with entries in a *field* was recently given in [7]: A is invertible if and only if both its rows and its columns are (infinitely) linearly independent.

Acknowledgement The author thanks referees for helpful remarks and for suggesting Example 1.

References

[1] Tom Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976, p. 127.

[2] Gerry Myerson, Solution for Problem 10185, *Amer. Math. Monthly*, 101(1994), p. 85.

[3] News and Letters, *Math. Magazine*, 69(1996), 233-238.

[4] Bjorn Poonen, Jim Propp, and Richard Stong, Problem 10553, *Amer. Math. Monthly*, 103(1996), p. 809.

[5] Pólya and Szegö, *Problems and Theorems in Analysis* II, Springer-Verlag, 1990, Chapter 8, Part 2, §1.

[6] Warren J. Wong, Powers of a Prime Dividing a Binomial Coefficient, *Amer. Math. Monthly*, 96(1989), 513-517.

[7] Shi Qiang Wang, The Inverses of Infinite Matrices over a Field, *Beijing Shifan Daxue Xuebao* 29(1993), no. 3, 327-330. MR **94k**:15003.

AMS Classification numbers: 15A36, 15A09, 15A03.