find this particular version in the literature. I would like to thank Milgram for pointing out the paper [1] which contains the theorem proved below. The proof in [1] makes use of Gauss' lemma rather than the norm calculation used here.

Let σ_p be a primitive pth root of 1 and set $K_p = \mathbb{R} \cap \mathbb{Q}(\sigma_p)$. The element $1 - \sigma_p$ is prime in $\mathbb{Q}(\sigma_p)$ with norm p. Let π_p be the norm of $1 - \sigma_p$ in K_p. Then $N(\pi_p) = p$ and $\pi_p = (1 - \sigma_p)(1 - \sigma_p^{-1}) = 2 - \sigma_p - \sigma_p^{-1}$. If p and q are primes consider $\eta = \pi_p - \pi_q$ in $L = K_pK_q$. It is a unit since $\eta = \sigma_q^{-1}(1 - \sigma_p\sigma_q)(1 - \sigma_p^{-1}\sigma_q)$. Since $\eta \equiv \pi_p \pmod{\pi_q}$, $N(\eta) \equiv N(\pi_p) \pmod{q}$. Now $N(\pi_p) = N_{K_p/Q}N_{L/K_p}(\pi_p) = N_{K_p/Q}(\pi_p^{(q-1)/2}) = p^{(q-1)/2} \equiv (p/q) \bmod q$ by Euler's criterion. But $N(\eta) = \pm 1$, so we have proved the following result.

THEOREM. *$N(\pi_p - \pi_q) = (p/q)$ for odd primes p and q.*

Interchanging p and q now gives quadratic reciprocity.

COROLLARY. *$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$ for odd primes p and q.*

When $q = 2$, we can consider instead $\tau = 2 - \pi_p = \sigma_p + \sigma_p^{-1}$ in K_p. The same argument gives $N(\tau) = (2/p)$ but switching p and 2 is useless. Instead consider $f_n = x^n + \cdots + 1 + \cdots + x^{-n} = g_n(z)$ where $z = x + x^{-1}$. Then $zg_n(z) = g_{n-1}(z) + g_{n+1}(z)$ so $g_{n+1}(0) = -g_{n-1}(0)$ showing that $g_n(0) = 1$ for $n \equiv 0, 1 \bmod 4$ and $g_n(0) = -1$ otherwise. Since g_n is the minimal polynomial of τ for $n = (p - 1)/2$, we see that $(2/p) = N(\tau) = (-1)^n g_n(0) = (-1)^{(p^2-1)/8}$ as required.

REFERENCES

1. M. Gerstenhaber, The 152-nd proof of the law of quadratic reciprocity, this MONTHLY, 70 (1963) 397–398.
2. R. J. Milgram, Odd index subgroups of units in cyclotomic fields and applications, Springer Lecture Notes 854, 1980, pp. 269–298.

Adding up to Powers

EDWARD A. BENDER
Department of Mathematics, University of California—San Diego, La Jolla, CA 92093

FRED KOCHMAN
Institute for Defense Analyses, Princeton, NJ 08540

DOUGLAS B. WEST
Department of Mathematics, University of Illinois, Urbana, IL 61801

Here is a short combinatorial proof that a somewhat mysterious way of generating the kth powers of the natural numbers actually works. It generalizes the well-known fact that the sum of the first n odd numbers is n^2. The proof makes a nice presentation in an introductory combinatorics course. It uses recurrence relations, proof by 1-1 correspondence, and counting of lattice paths in a problem that students are likely to find appealing.

After discussing the kth powers, we will discuss a generalization of this procedure. We can still explain the resulting numbers as values of polynomials. We will see, however, that generating the kth powers is a very special case.

1. Generating the Perfect Powers. The procedure is as follows. Begin by writing down the natural numbers in sequence, calling this row 1. Next, strike out every kth term. Take partial sums of the surviving sequence to generate row 2. In general, generate row $j+1$ from row j by striking out every $k+1-j$th term and taking partial sums of the surviving sequence. The claim is that row k consists of precisely the kth powers of the natural numbers, in sequence. The procedure is illustrated below for $k = 4$. Note that the successive deletions make the numbers appear in wedges; a number is in wedge n if the first deletion to its right is the nth deletion in that row.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	3	6		11	17	24		33	43	54		67	81	96		113	131	150	
1	4			15	32			65	108			175	256			369	500		
1				16				81				256				625			

The numbers in the major diagonal of each wedge have a recognizable form. Let $a_{j,n}$ be the number in row j of the nth major diagonal. Then in fact $a_{j,n} = n^j\binom{k}{j}$. We prove this by showing that the $a_{j,n}$ and the numbers $b_{j,n} = n^j\binom{k}{j}$ satisfy the same recurrence. First we study the $b_{j,n}$.

LEMMA 1. *The values* $b_{j,n} = n^j\binom{k}{j}$ *satisfy the recurrence* $b_{j,n} = \sum_{i=1}^{j}\binom{k-i}{j-i}b_{i,n-1}$.

Proof. Consider the sequences formed from the integers $\{0,\dots,n\}$. Let $S_{k,j}$ be the sequences that have k terms, of which j are nonzero. Both sides of the claimed equality count $S_{k,j}$. To show $|S_{k,j}| = n^j\binom{k}{j}$, simply choose the positions for the non-zero entries and fill them in. To show the sum also counts $S_{k,j}$, partition $S_{k,j}$ by the number of positions containing terms greater than 1. This number may be anywhere from 0 to j; if it is i, the positions of terms exceeding 1 can be chosen in $\binom{k}{i}$ ways, the positions can be filled in $(n-1)^i$ ways, and the $j-i$ 1's can be placed in $\binom{k-i}{j-i}$ ways. □

To prove the desired theorem, we need only verify the initial conditions and show that the $a_{j,n}$ satisfy the same recurrence. First, we need a row corresponding to $j = 0$. So, add a 0th row to the display, consisting entirely of 1's. In particular, $a_{0,n} = 1$. The wedge $n = 0$ is entirely 0 except $a_{0,0} = 1$.

THEOREM 1. $a_{j,n} = n^j\binom{k}{j}$.

Proof. The proof is by induction; we have already verified the basis. We need only show $a_{j,n} = \sum_{i=0}^{j}\binom{k-i}{j-i}a_{i,n-1}$ for $n \geq 1$. Note that every entry in the display is the sum of the entry to its left and the entry above it. If we imagine an $a-1$th row consisting of 0's, this means every $a_{j,n}$ can be broken down into contributions from entries in the main diagonal of the $n-1$st wedge. We need only determine how many times each $a_{i,n-1}$ contributes to each $a_{j,n}$. This is precisely the number of paths from $a_{i,n-1}$ to $a_{j,n}$ that always move rightward or downward at each step.

Due to the deletions in each row, there is no element below $a_{i,n-1}$, so every path from $a_{i,n-1}$ must take its first step to the right. From there, the paths to $a_{j,n}$ are precisely the lattice paths counted by the appropriate binomial coefficients. These paths enter the nth wedge in the ith diagonal, and they end at the kth diagonal, so the total number of steps is $k - i$. The number of steps downward is $j - i$, so the correct coefficient is indeed $\binom{k-i}{k-j}$. (In fact, more generally, the jth entry in the lth diagonal of the nth wedge is $\sum_{i=0}^{j}\binom{l-i}{j-i}n^j\binom{k}{j}$.) □

In particular, $a_{k,n} = n^k$, as desired.

2. A Generalization. The procedure generating the powers can be generalized to yield other polynomials. As before, begin with row 0 having a 0 in position 0 and 1's thereafter. At row j, choose a modulus m_j and a remainder r_j with $1 \leqslant r_j \leqslant m_j$. Create row $j + 1$ by 1) deleting from row j the entries $r_j + sm_j$ for $s \geqslant 0$, and 2) computing partial sums of what remains. We call this the *addition procedure*. Row 1 is always the natural numbers, so we don't bother to specify m_0, r_0. To generate the powers of the natural numbers, we used the addition procedure with $m_j = k + 1 - j$ and $r_j = m_j$. We claim that, for any choice of $\{m_j\}$ and $\{r_j\}$, the sequence arising at each row consists of the values of a finite number of polynomials, evaluated at consecutive integers. To prove this, we first review elementary facts about polynomials and binomial coefficients.

LEMMA 2. *Any polynomial $p(n)$ of degree j has a unique expression as a linear combination of $\binom{n}{0}, \ldots, \binom{n}{j}$.*

Proof. If the leading coefficient of $p(n)$ is c, let the coefficient of $\binom{n}{j}$ be $j!c$ and apply induction. □

LEMMA 3. *If a, b are constants and p is a polynomial of degree j with leading coefficient c, then $\sum_{s=0}^{t} p(as + b)$ is a polynomial in t of degree $j + 1$ with leading coefficient $ca^j/(j + 1)$.*

Proof. The expression $p(as + b)$ is a polynomial of degree j in s. Using the preceding lemma (and its proof), we express it as $\sum_{i=0}^{j} c_i\binom{s}{i}$, with $c_j = ca^j j!$. By interchanging the order of summation and applying the fundamental combinatorial identity $\sum_{s=0}^{t}\binom{s}{i} = \binom{t+1}{i+1}$, the desired sum becomes $\sum_{i=0}^{j} c_i\binom{t+1}{i+1}$. This is a polynomial in t of degree $j + 1$, with leading coefficient $c_j/(j + 1)! = ca^j/(j + 1)$. □

We say that a sequence $b_1, \ldots$ is a *polynomial sequence of degree k* if $b_i = p(i)$ for $1 \leqslant i \leqslant n$ for some polynomial p of degree k.

THEOREM 2. *Let $\{(r_j, m_j)\}$ be an instance of the addition procedure. For each j, there is a modulus M_j such that the congruence classes of positions mod M_j partition row j into polynomial subsequences of degree j. Furthermore, the leading coefficients of these polynomials are equal and depend only on $(m_1, \ldots, m_j)$.*

Proof. We prove this by induction on j; for $j = 1$ we may choose $M_1 = 1$ and the polynomial $p(i) = i$.

Consider $j \geqslant 1$, and suppose the claim holds for row j with polynomials $p_0, \ldots, p_{M_j - 1}$ having leading coefficients c. Let f_i denote the ith element of row $j + 1$. Let $a = \operatorname{lcm}(M_j, m_j)$, and define $M_{j+1} = a(1 - 1/m_j)$. Fix an integer r with

$0 \leqslant r < M_j$, and consider the subsequence $g_s = f_{sM_j+r}$. The difference $g_{s+1} - g_s$ is composed of contributions from the polynomials $\{p_l\}$. The choice of M_{j+1} accounts for the deletions from row j so that the pattern of contributions to $g_{s+1} - g_s$ from elements explained by a given p_l is the same for each value of s. Each polynomial p_l contributes a consecutive segment of its values, except that gaps arise due to deletions from row j. In particular, the contribution from p_l has the form $\sum_{i=1}^{d} p_l(n + \alpha_i)$, where $d \leqslant a/M_j$, the α_i's are d of the first a/M_j natural numbers, and the omissions depend only on r and l. For any value of n, this is the sum of d jth-degree polynomials in n. Hence it also has degree j, and it has leading coefficient dc.

The value of n used in this polynomial to compute the contribution of p_l to $g_{s+1} - g_s$ is $(a/M_j)s + \lfloor r/M_j \rfloor$. The contribution to $g_t - g_0$ from p_l is thus a partial sum of equally-spaced terms from a polynomial sequence of degree j. By the lemma, the sum is a polynomial in t of degree $j + 1$, with leading coefficient $dc(a/M_j)^j/(j + 1)$. Finally, we collect the contributions to g_t from all p_l and add the constant $g_0 = f_r$ to express g_s as a polynomial in s of degree $j + 1$. The leading coefficient is $c(a/M_j)^j/(j + 1)$ times the sum of the values d associated with the various p_l's. This sum is always M_{j+1}, because it equals the number of elements of row j added in to increase g_s to g_{s+1}. This completes the induction. □

With $M_1 = 1$ and $M_{j+1} = \operatorname{lcm}(M_j, m_j) \cdot (m_j - 1)/m_j$ as in the proof, we conclude that the leading coefficient for the polynomials explaining row j is $(1/j!)\prod_{i=1}^{j-1} M_{i+1}(\operatorname{lcm}(M_i, m_i)/M_i)^i$.

3. Additions and Differences. In the special case considered in Section 1, the polynomial $b_j(n) = \binom{k}{j} n^j$ is precisely the polynomial generated by the above procedure for row j when $m_j = r_j = k + 1 - j$ for $j = 1, \ldots, k$.

As another example, consider the addition procedure with $m_1 = 3$, $r_1 = 2$, $m_2 = 5$, $r_2 = 3$. The first three rows of the resulting display are

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17...
0	1		4	8		14	21		30	40		52	65		80	96	...
0	1		5			19	40		70	110			175		255	351	...

Taking the polynomial n for row 1, the two polynomials obtained for row 2 are $6\binom{n}{2} + 4n = 3n^2 + n$ and $6\binom{n}{2} + 7n + 1 = 3n^2 + 4n + 1$. In passing from row 2 to row 3, the pattern of deletions versus usage of polynomials repeats after 8 surviving terms of row 3, because $8 = \operatorname{lcm}(2, 5) \cdot (4/5)$. Thus eight polynomials suffice to explain the elements of row 3; the first two are $1200\binom{n}{3} + 1300\binom{n}{2} + 255n$ and $1200\binom{n}{3} + 1450\binom{n}{2} + 350n + 1$.

Note that we expressed these polynomials in terms of binomial coefficients. Once we know which values are covered by one of these polynomials, we can obtain the full polynomial quickly from $j + 1$ elements of row j by using the method of repeated differencing. Take the first $j + 1$ values of one congruence class mod M_j, the first of which will be the value of the desired polynomial at $n = 0$. Take the differences of consecutive values to get a sequence of j values. Continue this differencing to produce successively shorter sequences, the $j + 1$th sequence having only a single value. Let $c_0, \ldots, c_j$ denote the initial values in these $j + 1$ successive difference sequences. It is easily proved by induction that the tth difference

sequence consists of the first $j + 1 - t$ values of the polynomial $\Sigma_{i \geqslant t} c_i \binom{n}{i-t}$. In particular, the polynomial giving the initial sequence is $\Sigma c_i \binom{n}{i}$.

At this point, the curious reader will wonder what polynomials can arise from this procedure. In general, this appears to be difficult. However, suitable restrictions of the question yield interesting results.

First, note that winding up with a single polynomial as we did in Section 1 is a fairly special occurrence; it seems to require $M_k = 1$. Nevertheless, we can always guarantee it by choosing $m_j = k + 1 - j$. This still leaves a fair amount of variability in the choice of r_j, but since $0 \leqslant r_j < m_j$, this limits us to at most $k!$ polynomials for each value of k. Furthermore, the computation in the proof of Theorem 2 shows that these are all monic polynomials, which makes this class even more interesting.

Using the differencing procedure and the relationship between $\{\binom{n}{i}\}$ and $\{n^i\}$ via the Stirling numbers, it is a pleasant exercise to calculate some of these polynomials. For $k = 2$ the two polynomials are n^2 and $n^2 + n$. For $k = 3$, the six polynomials can be described concisely; n^3 has a different form from the other five, which are $n^3 + j(n^2 + n)/2 - n$, for $j = 1, 2, 3, 4, 5$. For $n = 4$, more formulas are necessary to explain all the polynomials, and the polynomials are not all distinct. We will close by listing those for which all coefficients are integers.

r_1	r_2	r_3	n^4	n^3	n^2	n
4	3	2	1			
1	3	2	1	1		
4	3	1	1	2	1	
3	2	1	1	3	3	1
2	1	2	1	2	1	
2	1	1	1	4	5	2

The appearance of the pure powers no longer looks quite so strange. Certainly there are some patterns here that are worth exploring.

Note added in proof: We have learned from C. T. Long and from this MONTHLY, 95 (1988) 708 that the process of our Section 1 is called Moessner's process and has been known since 1951. See Long's paper in this MONTHLY, 73 (1966) 846–851, for references and a proof of a certain generalization, different from our generalization.