AN APPLICATION OF PARTITIONS TO THE FACTORIZATION OF POLYNOMIALS OVER FINITE FIELDS

Julia Varbalow and David C. Vella
University of Kentucky and Skidmore College

In this paper, partitions of natural numbers are used to count the irreducible polynomials of degree n over a finite field. This apparently little known application of partitions is described in detail in Section II. Section I is a brief introduction to partitions. These results were developed as part of the first author's senior mathematics thesis under the direction of the second author.

I) Introduction. Let n be a natural number. A partition of n is a finite set π of natural numbers (possibly with repetitions) whose sum is n. We sometimes write $\pi \vdash n$ to indicate that π is a partition of n. For example if $\pi = \{4, 3, 3, 1, 1, 1\}$, then $\pi \vdash 13$. Two partitions are considered equal if they have the same entries or *parts*, regardless of the order of those parts. For convenience, partitions are frequently written with their parts in nonincreasing order: $\pi = \{p_1, p_2, \ldots, p_m\}$ where $p_1 \geq p_2 \geq \cdots \geq p_m$, as in the above example.

For each i $(1 \leq i \leq n)$, the number of times i occurs as a part of the partition π is called the *multiplicity* of i in π, and is denoted by $m_i(\pi)$ or more simply by π_i (so π_i is the cardinality of $\{p_k \mid p_k = i\}$). This leads to an alternate notation for partitions where π is denoted by $[1^{\pi_1}, 2^{\pi_2}, \ldots, n^{\pi_n}]$ with entries of multiplicity zero omitted. Thus the above partition π of 13 can also be written as $[1^3, 3^2, 4]$, suppressing the superscripts equal to 1. We shall refer to the number of parts $\ell(\pi)$ of π as its *length* and the number of distinct parts $d(\pi)$ as its *depth*. In the above example $\pi = [1^3, 3^2, 4]$, we have $\ell(\pi) = 6$ and $d(\pi) = 3$. It is clear that the length of any partition is the sum of the multiplicities of its parts:

$$\ell(\pi) = \sum_{i=1}^{n} \pi_i \quad \text{if} \quad \pi \vdash n. \tag{1}$$

Let P stand for the set of all partitions. Let $P_n = \{\gamma \in P \mid \gamma \vdash n\}$ be the set of partitions of n, so $P = \bigcup_{n=1}^{\infty} P_n$ (disjoint union). It will be convenient to allow the number 0 to be a part of a partition. In fact, although we will omit 0 when writing a partition, we will follow the convention of assuming that 0 is a part of any partition, of multiplicity 1, although it contributes nothing to the length or the depth of the partition. Thus $m_0(\pi) = \pi_0 = 1$ for all $\pi \in P_n$, while the sum in (1) is *not* adjusted to begin at $i = 0$. Furthermore, in order to treat the formulas appearing in Section II uniformly, it will also be convenient to assume there is precisely one partition of 0 (which has length 0 and depth 0), namely $[0]$, which we adjoin to P.

The *partition function* is defined by $p(n) = |P_n|$ (cardinality of P_n). For example $p(5) = 7$, since

$$P_5 = \{[5], [1, 4], [2, 3], [1^2, 3], [1, 2^2], [1^3, 2], [1^5]\}.$$

One may compute $p(n)$ for small values of n by hand, although this process soon becomes tedious since $p(n)$ grows rather quickly. For instance, $p(10) = 42$, $p(20) = 627$, and $p(100) = 190{,}569{,}292$. While there is an exact formula for $p(n)$ (see [7]), it is rather complicated and many calculations of $p(n)$ rely instead on some kind of recursion.

The partition function and partitions in general have a long history, and they arise in many diverse situations. The grade school student may meet them in simple counting exercises such as "how many ways are there to make change for a dollar without pennies?", which is really the question of how many partitions of 100 are there with each part equal to 5, 10, 25, or 50. In a similar manner one can rephrase questions such as "how many different ways are there to roll a 12 with exactly three dice?" or "what is the largest number of Chicken McNuggets that you cannot order exactly if they come in packages of 6, 9, and 20?". The reader should have no trouble seeing that these questions and many others like them are really questions about counting partitions with certain restrictions on the parts. While these questions can be answered easily by ad hoc methods, a very satisfying

uniform method exists which is sometimes covered in an introductory course in discrete mathematics. Originally due to Euler, it is based on multiplying together certain power series (e.g., see [4], section 19.3) known as *generating functions*.

Like the above examples, many of the most interesting problems related to partitions involve counting partitions with restrictions on the parts. However, just as $p(n)$ itself is elusive, it is frequently impossible to do this directly with the added restrictions. As a consequence, many counting arguments focus on showing that one set of restricted partitions is equinumerous with a different set of restricted partitions without actually counting either set. For example, it is a well known result that the number of partitions of n into at most k parts is the same as the number of partitions of n into parts which are at most k. As a concrete example consider the case $n = 6$, $k = 3$. The partitions of 6 into parts which are at most 3 are

$$\{[1^6], [1^4, 2], [1^2, 2^2], [2^3], [1^3, 3], [1, 2, 3], [3^2]\}$$

and the partitions of 6 into at most 3 parts are

$$\{[6], [1, 5], [2, 4], [3^2], [1^2, 4], [1, 2, 3], [2^3]\}.$$

There are the same number of partitions in each set, namely seven.

The interested reader will find an elegant proof of this assertion (and many others like it) using a graphical device known as the Ferrers diagram of a partition (invented by N. M. Ferrers and later popularized by J. J. Sylvester) in [1].

In addition to these counting problems there are many celebrated applications of partitions in other areas of mathematics. Two of our favorites in group theory are the connection between partitions of n and the conjugacy classes in the symmetric group S_n and the classification theorem of finite Abelian groups. Since these applications can be found in any good introduction to abstract algebra ([6], for example), we will not dwell on them. At a somewhat deeper level there are also some beautiful applications to the representation theory of S_n (see [8]). Partitions of a natural number can also be used to extend the chain rule of calculus to higher derivatives, leading to the well-known Bell polynomials (see [3]), among other things. The interested reader can find some applications of this in [12]. We will presently describe an application of partitions to undergraduate mathematics which does not seem to be as widely known.

II) Counting Irreducible Polynomials Over Finite Fields.

Let F be a field and let $F[X]$ be the ring of polynomials with coefficients in F. Then $F[X]$ is a unique factorization domain, and the nonzero constant polynomials form the group of units (see [5], [6], or [10]). Thus, every polynomial of degree 1 or larger factors into a product of a nonzero constant and monic irreducible polynomials in a unique way (up to the order of the factors), where *monic* means the leading coefficient is 1. Thus in many ways this ring behaves like the ring Z of integers. In particular, the (monic) irreducible polynomials play the role of the (positive) prime numbers in Z.

Therefore, one could ask questions about the distribution of irreducible monic polynomials which are analogous to questions about the distribution of primes in Z. Because $F[X]$ is an integral domain, the degree of $p(X)q(X)$ is the sum of the degrees of $p(X)$ and $q(X)$. By induction on m, the following is true:

$$\deg\left(\prod_{i=1}^{m} p_i(X)\right) = \sum_{i=1}^{m} \deg(p_i(X)). \tag{2}$$

It follows that every (monic) polynomial of degree one is irreducible. Such a polynomial has the form $X + a$ for some $a \in F$, so if F is infinite, the ring $F[X]$ has an infinite number of irreducible polynomials just as Z has an infinite number of primes. (In case F is algebraically closed, these are the only monic irreducible polynomials.) It turns out that even if F is a finite field, there are still infinitely many irreducible polynomials (see page 274 of [5] for the case $F = Z_p$, the field of integers modulo the prime p), although there can be only a finite number of any fixed degree n. This raises the question of finding the number of irreducible polynomials of each degree in case F is finite.

Let $N_F(n)$ stand for the number of irreducible monic polynomials of degree n over the field F. In case F is a finite field with q elements (where $q = p^r$, p is the characteristic of F), we will also use the standard notation $N_q(n)$. Our method for computing $N_F(n)$ is a recursive method based on (2). It is a generalization of exercise C, page 255 of [10], except that there

it is only carried out for $n = 2$ and $n = 3$. When this is attempted for larger values of n, partitions enter the picture. Indeed, if $p(X)$ is a monic polynomial of degree n, it factors uniquely as a product of monic irreducible polynomials $p(X) = \Pi_{i=1}^{m} p_i(X)$. So if we let $d_i = \deg(p_i(X))$, then (2) implies that the set of degrees $\{d_1, d_2, \cdots, d_m\}$ is a partition of n. Furthermore, $p(X)$ is itself irreducible only if the partition so obtained is $[n]$, otherwise each $d_i < n$. A typical monic polynomial of degree n has the form

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0,$$

with the a_i's in F. Let F be finite from now on, with $q = |F|$. Now there are exactly q choices for each of the n a_i's, so there are q^n monic polynomials of degree n altogether. Our goal is to count the number of reducible polynomials of degree n (provided $N_F(d_i)$ for $d_i < n$ has already been computed), and subtract this number from q^n to find $N_F(d_i)$.

First we consider some preliminary information regarding partitions. We remind the reader that the conventions about 0 from Section I are still in effect. We now introduce an operation on P. Given a partition $\pi \vdash n$, recall that the length $\ell(\pi)$ is the total number of (nonzero) parts and the depth $d(\pi)$ is the number of distinct (nonzero) parts. From (1) it follows that the set of multiplicities $\delta(\pi) = \{\pi_1, \pi_2, \cdots, \pi_n\}$ is a partition of $\ell(\pi)$, which we call the *derived partition* of π. Observe that $\delta(\pi)$ has length equal to the depth of π (many of the multiplicities π_i are 0). For example, if $\pi = [1^3, 2, 4^2, 5^3]$, then $\pi \vdash 28$ and there are 9 parts, but only 4 of them are distinct, so $\ell(\pi) = 9$ and $d(\pi) = 4$. The multiplicities are $\{3, 1, 0, 2, 3\}$, leading to $\delta(\pi) = [1, 2, 3^2]$, a partition of 9 of length 4. We further illustrate this with the table on the next page.

Next, suppose that $\pi \in P_n$; $\pi = \{p_1, p_2, \cdots, p_m\}$. Then we remind the reader that the expression $n! \Big/ \Pi_{i=1}^{m} p_i!$ is an integer, known as a multinomial coefficient, and often written as $\begin{bmatrix} n \\ p_1, p_2, \cdots, p_m \end{bmatrix}$. We will further abbreviate this to simply $\begin{pmatrix} n \\ \pi \end{pmatrix}$, writing the name of the partition on the bottom. When $m = 2$, we will follow the usual convention of writing the binomial coefficient as $\begin{bmatrix} n \\ p_i \end{bmatrix}$ rather than $\begin{bmatrix} n \\ p_1\ p_2 \end{bmatrix}$ or $\begin{pmatrix} n \\ \pi \end{pmatrix}$.

Derived partitions for P_4

π	π_i i: 1,2,3,4	$\ell(\pi)$	$\delta(\pi)$	$d(\pi) = \ell(\delta(\pi))$
4	0,0,0,1	1	1	1
3,1	1,0,1,0	2	1, 1	2
2,2	0,2,0,0	2	2	1
2,1,1	2,1,0,0	3	2, 1	2
1,1,1,1	4,0,0,0	4	4	1

We are now prepared to prove the following:

THEOREM 1: Let F be a finite field with $|F| = q$. Then the total number of monic polynomials of degree n with coefficients in F is given by:

$$(3) \qquad q^n = \sum_{\pi \in P_n} \left[\prod_{j=1}^{n} \left[\sum_{\beta \in P_{\pi_j}} \begin{bmatrix} N_q(j) \\ \ell(\beta) \end{bmatrix} \cdot \begin{bmatrix} \ell(\beta) \\ \delta(\beta) \end{bmatrix} \right] \right]$$

Proof: We have observed above that the left side of (3) is correct. We now count the monic polynomials a different way to see that the right side is also correct. Let $p(X)$ be one, and let $p(X) = \Pi_{i=1}^{m} p_i(X)$ be its factorization into irreducible monic polynomials. Let π be the degree set $\{d_1, d_2, \cdots, d_m\}$ (listed with multiplicities). Since $F[X]$ is a commutative ring, the d_i's may be listed in any order, so as noted above, π belongs to P_n. Let j be an integer with $1 \le j \le n$. So there are π_j of the irreducible factors $p_i(X)$ with degree j. If N_j represents the number of ways of choosing these factors of degree j, then the multiplication principle of counting yields that there are $\Pi_{j=1}^{n} N_j$ ways of choosing all the factors together, so this accounts for the product in (3).

It remains to show that

$$N_j = \sum_{\beta \in P_{\pi_j}} \begin{bmatrix} N_q(j) \\ \ell(\beta) \end{bmatrix} \cdot \binom{\ell(\beta)}{\delta(\beta)}.$$

First observe that for a given value of j, it may be the case that none of the $p_i(X)$'s have degree j, so that particular factor N_j should have a value of 1. But if there are no factors of degree j, then $\pi_j = 0$ and so the innermost sum runs over the index set $P_0 = \{[0]\}$. Thus there is only one summand corresponding to the partition [0] of 0. By our conventions about zeros, both the length and the depth of the partition [0] are 0, so that both the binomial and the multinomial coefficient have the value 1, as desired.

So now consider the case where $\pi_j > 0$, so there is at least one of the $p_i(X)$'s with degree j. Now there are exactly $N_q(j)$ monic irreducible polynomials of degree j to choose from, and we must choose exactly π_j of them, possibly with repetitions, for the $p_i(X)$'s of degree j. The possibility of repetitions complicates matters, so we break the problem into two steps. First, select the distinct factors, and second select their multiplicities to add up to π_j, the total number of factors of degree j. Since their multiplicities add up to π_j (and again the order of the factors is irrelevant), the set of such multiplicities $\beta = \{\mu_1, \mu_2, \cdots, \mu_r\}$ forms a partition of π_j of length $\ell(\beta) = d$ equal to the number of distinct factors. Conversely, every partition of π_j accounts for a possible set of multiplicities for the factors of degree j. This is why the innermost sum runs over P_{π_j}.

Now given a partition β of π_j, since $d = \ell(\beta)$ is the number of distinct factors, the binomial coefficient $\begin{bmatrix} N_q(j) \\ d \end{bmatrix}$ counts all the possible sets of distinct factors from among the $N_q(j)$ which are available. For each such set, the multinomial coefficient $\begin{pmatrix} d \\ \beta_1 \beta_2 \cdots \beta_{\pi_j} \end{pmatrix}$ counts the number of ways of assigning the given multiplicities to that particular set of factors, where β_k is the multiplicity of k as a part of β. (That is, β_k is the number of distinct factors (of degree j) which have multiplicity k.) But observe that the set $\{\beta_1, \beta_2, \cdots, \beta_{\pi_j}\}$ is nothing more than the derived partition $\delta(\beta)$ of β. Thus N_j has the desired form and this completes the proof of the theorem.

COROLLARY 1: Let F be a finite field with $|F| = q$. Then the number $N_q(n)$ of monic irreducible polynomials of degree n can be computed recursively from the formula

$$(4) \quad N_q(n) = q^n - \sum_{\substack{\pi \in P_n \\ \ell(\pi) > 1}} \left(\prod_{j=1}^{n} \left(\sum_{\beta \in P_{\pi_j}} \begin{bmatrix} N_q(j) \\ \ell(\beta) \end{bmatrix} \cdot \binom{\ell(\beta)}{\delta(\beta)} \right) \right).$$

Proof: Formula (4) follows immediately from (3) because the only partition in P_n of length 1 is $[n]$, which corresponds to the case of $p(X)$ being irreducible in Theorem 1. It is recursive because $\ell(\pi) > 1$ implies that $\pi_n = 0$, whence the only $N_q(j)$'s which appear in the right hand side are those for which $j < n$.

Some examples may help to clarify what we have done. First, we show a specific example of the counting technique used in the proof of Theorem 1. Suppose that $p(X)$ is a degree 24 polynomial, with factorization $P(X) = \Pi_{i=1}^{9} p_i(x)$, with one linear factor, three quadratic factors, four cubic factors, and one quintic factor. This corresponds to the partition $\pi = [1, 2^3, 3^4, 5]$ of 24 in the outermost sum of (3). There are 24 factors N_j in the product, but since $\pi_4 = 0$ and $\pi_j = 0$ for $6 \le j \le 24$, most of these factors have the value 1. By definition there are $N_q(1) = q$ ways to choose the linear factor and $N_q(5)$ ways to choose the quintic factor. Consider next the quadratic factors. Since $\pi_2 = 3$, the index set for the innermost sum of (3) is $P_3 = \{[1^3], [1, 2], [3]\}$.

The partition $\beta = [1^3]$ corresponds to choosing three distinct (quadratic) factors, since $\ell(\beta) = 3$. Since there are only three quadratic factors altogether, each of these three necessarily occurs with multiplicity 1 (the parts of β), so there is only one way to assign these multiplicities. Observe that $\delta([1^3])$ is the partition [3], since $\beta_1 = 3$, $\beta_2 = 0$, $\beta_3 = 0$. Thus the number of ways to choose 3 distinct quadratic factors is

$$\begin{bmatrix} N_q(2) \\ \ell(\beta) \end{bmatrix} \cdot \binom{\ell(\beta)}{\delta(\beta)} = \begin{bmatrix} N_q(2) \\ 3 \end{bmatrix} \cdot \binom{3}{3, 0, 0} = \begin{bmatrix} N_q(2) \\ 3 \end{bmatrix} \cdot 1.$$

The partition $\beta = [1, 2]$ corresponds to choosing two distinct (quadratic) factors, since $\ell(\beta) = 2$. One of them will have multiplicity 1 and one will have multiplicity 2 (the parts of β), and clearly there are exactly two ways to make that assignment. Observe that the derived

partition in this case is $\delta(\beta) = [1^2]$, since $\beta_1 = \beta_2 = 1$ and $\beta_3 = 0$. Thus the number of ways to choose two distinct factors with one repeated twice is

$$\begin{bmatrix} N_q(2) \\ \ell(\beta) \end{bmatrix} \cdot \binom{\ell(\beta)}{\delta(\beta)} = \begin{bmatrix} N_q(2) \\ 2 \end{bmatrix} \cdot \binom{2}{1, 1, 0} = \begin{bmatrix} N_q(2) \\ 2 \end{bmatrix} \cdot 2 .$$

Finally the partition [3] of length 1 corresponds to choosing exactly one (quadratic) factor and using it three times (there is only one way to assign the multiplicity). In this case the derived partition is [1] as $\beta_1 = \beta_2 = 0$ and $\beta_3 = 1$. Thus

$$\begin{bmatrix} N_q(2) \\ \ell(\beta) \end{bmatrix} \cdot \binom{\ell(\beta)}{\delta(\beta)} = \begin{bmatrix} N_q(2) \\ 1 \end{bmatrix} \cdot \binom{1}{0, 0, 1} = \begin{bmatrix} N_q(2) \\ 1 \end{bmatrix} \cdot 1 .$$

This shows that in this case

$$N_2 = \begin{bmatrix} N_q(2) \\ 3 \end{bmatrix} \cdot 1 + \begin{bmatrix} N_q(2) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_q(2) \\ 1 \end{bmatrix} \cdot 1 .$$

Similarly, for the $\pi_3 = 4$ cubic factors, one may compute N_3 as a sum over P_4. Using the table above of the derived partitions for all $\pi \vdash 4$, one obtains $N_3 =$

$$\begin{bmatrix} N_q(3) \\ 4 \end{bmatrix} \cdot 1 + \begin{bmatrix} N_q(3) \\ 3 \end{bmatrix} \cdot 3 + \begin{bmatrix} N_q(3) \\ 2 \end{bmatrix} \cdot 1 + \begin{bmatrix} N_q(3) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_q(3) \\ 1 \end{bmatrix} \cdot 1 .$$

Therefore, the total number of degree 24 monic polynomials which factor into monic irreducible polynomials with degrees corresponding to the partition $\pi = [1, 2^3, 3^4, 5]$ is

$$\prod_{j=1}^{24} N_j = N_1 \cdot N_2 \cdot N_3 \cdot 1 \cdot N_5 \cdot \cdots \cdot 1 =$$

$$\begin{bmatrix} N_q(1) \\ 1 \end{bmatrix} \cdot \left[\begin{bmatrix} N_q(2) \\ 3 \end{bmatrix} + \begin{bmatrix} N_q(2) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_q(2) \\ 1 \end{bmatrix} \right] \cdot$$

$$\left[\begin{bmatrix} N_q(3) \\ 4 \end{bmatrix} + \begin{bmatrix} N_q(3) \\ 3 \end{bmatrix} \cdot 3 + \begin{bmatrix} N_q(3) \\ 2 \end{bmatrix} \cdot 3 + \begin{bmatrix} N_q(3) \\ 1 \end{bmatrix} \right] \cdot \begin{bmatrix} N_q(5) \\ 1 \end{bmatrix} .$$

Of course, there are many other partitions of 24 to consider! Let us close

with an example of the corollary. Let $F = Z_p$ so that $q = p$, and let $n = 5$. Then (3) becomes

$$p^5 = \begin{bmatrix} N_p(5) \\ 1 \end{bmatrix} + \begin{bmatrix} N_p(4) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_p(1) \\ 1 \end{bmatrix} +$$

$$\begin{bmatrix} N_p(3) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_p(2) \\ 1 \end{bmatrix} +$$

$$\begin{bmatrix} N_p(3) \\ 1 \end{bmatrix} \cdot \left[\begin{bmatrix} N_p(1) \\ 1 \end{bmatrix} + \begin{bmatrix} N_p(1) \\ 2 \end{bmatrix} \right] +$$

$$\left[\begin{bmatrix} N_p(2) \\ 1 \end{bmatrix} + \begin{bmatrix} N_p(2) \\ 2 \end{bmatrix} \right] \cdot \begin{bmatrix} N_p(1) \\ 1 \end{bmatrix} +$$

$$\begin{bmatrix} N_p(2) \\ 1 \end{bmatrix} \cdot \left[\begin{bmatrix} N_p(1) \\ 3 \end{bmatrix} + \begin{bmatrix} N_p(1) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_p(1) \\ 1 \end{bmatrix} \right] +$$

$$\begin{bmatrix} N_p(1) \\ 5 \end{bmatrix} + \begin{bmatrix} N_p(1) \\ 4 \end{bmatrix} \cdot 4 + \begin{bmatrix} N_p(1) \\ 3 \end{bmatrix} \cdot 3 + \begin{bmatrix} N_p(1) \\ 3 \end{bmatrix} \cdot 3$$

$$\begin{bmatrix} N_p(1) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_p(1) \\ 2 \end{bmatrix} \cdot 2 + \begin{bmatrix} N_p(1) \\ 1 \end{bmatrix} .$$

Notice that the number $N_p(5)$ occurs only in the first term, which corresponds to the sole partition [5] of length 1 in P_5. Specialize to the case $p = 3$. Then $N_3(1) = 3$, $N_3(2) = 3$, $N_3(3) = 8$, and $N_3(4) = 18$, as can be verified by using (3). Alternatively, one could look them up in a table (such as what appears in [9]), or use the approach outlined in [11]. Then the above expression for p^5 simplifies to

$$3^5 = \begin{bmatrix} N_3(5) \\ 1 \end{bmatrix} + \binom{18}{1} \cdot \binom{3}{1} + \binom{8}{1} \cdot \binom{3}{1} +$$

$$\binom{8}{1} \cdot \left[\binom{3}{1} + \binom{3}{2} \right]$$

$$+ \left[\binom{3}{1} + \binom{3}{2} \right] \cdot \binom{3}{1} + \binom{3}{1} \cdot \left[\binom{3}{3} + \binom{3}{2} \cdot 2 + \binom{3}{1} \right]$$

$$+ \binom{3}{5} + \binom{3}{4} \cdot 4 + \binom{3}{3} \cdot 3 + \binom{3}{3} \cdot 3 + \binom{3}{2} \cdot 2 + \binom{3}{2} \cdot 2 + \binom{3}{1} .$$

or, evaluating the binomial coefficients,

$243 = N_3(5) + 54 + 24 + 48 + 18 + 30 + 0 + 0 + 3 + 3 + 6 + 6 + 3$, which yields $N_3(5) = 243 - 195 = 48$. This checks with Table C, page 555 of [9].

Readers familiar with combinatorial arguments may have noticed a somewhat more direct way to compute N_j. Indeed, the binomial coefficient $\begin{bmatrix} n+s-1 \\ n \end{bmatrix}$ counts "combinations with repetition", i. e., it counts the number of ways of selecting (when order is irrelevant) n objects from a set of s objects where there is no restriction on the number of times a particular object may be repeated in the selection (see theorem 4.2 of [4], for example).

Now, there are precisely $N_q(j)$ factors of degree j available, and π_j of them must be selected (with possible repetitions, and without regard for order), so $N_j = \begin{bmatrix} N_q(j) + \pi_j - 1 \\ \pi_j \end{bmatrix}$. Thus, we have the following simplified version of (3)

$$q^n = \sum_{\pi \in P_n} \left[\prod_{j=1}^{n} \begin{bmatrix} N_q(j) + \pi_j - 1 \\ \pi_j \end{bmatrix} \right]. \tag{5}$$

Applying (5) to the case $p = q = 3$; $n = 5$ yields

$$3^5 = \begin{bmatrix} N_3(5) \\ 1 \end{bmatrix} + \begin{bmatrix} N_3(4) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_3(1) \\ 1 \end{bmatrix} + \begin{bmatrix} N_3(3) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_3(2) \\ 1 \end{bmatrix} + \begin{bmatrix} N_3(3) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_3(1)+1 \\ 1 \end{bmatrix} + \begin{bmatrix} N_3(2)+1 \\ 2 \end{bmatrix} \cdot \begin{bmatrix} N_3(1) \\ 1 \end{bmatrix} + \begin{bmatrix} N_3(2) \\ 1 \end{bmatrix} \cdot \begin{bmatrix} N_3(1)+2 \\ 3 \end{bmatrix} + \begin{bmatrix} N_3(1)+4 \\ 5 \end{bmatrix}$$

or, evaluating the binomial coefficients

$$243 = N_3(5) + 54 + 24 + 48 + 18 + 30 + 21,$$

which of course leads to the same value 48 for $N_3(5)$ computed above but is somewhat less tedious. While (5) is clearly more efficient than (3), the reason for giving both versions is to point out the connections with [2]. Indeed, one might distinguish the cases of factoring a quartic polynomial into either two distinct quadratics or one quadratic factor which is repeated by the notation "22" vs. "2^2". With this notation, it is clear that the 17 terms in the sum above obtained from (3) correspond to the 17 "factorization patterns" of 5: 5, 41, 32, 31^2, 311, 2^21, 221, 2111, 21^21, 21^3, 11111, 1^2111, 1^311, 1^21^21, 1^41, 1^31^2, 1^5. Thus, (3) will always reduce to a sum over the factorization patterns of n, while (5) will be a sum over the partitions of n. In [2], it is shown that the number of factorization patterns of n can be obtained by counting the partitions with "$d(a)$ copies of a". From our results, it is clear that each summand in (3) corresponds to a different factorization pattern of n, so it is immediate that one may obtain the number of factorization patterns of n by replacing each summand of the form

$$\begin{bmatrix} N_q(j) \\ \ell(\beta) \end{bmatrix} \cdot \begin{pmatrix} \ell(\beta) \\ \delta(\beta) \end{pmatrix}$$

by a 1. We obtain

COROLLARY 2 ([2], Lemma 2.1): Let $F(n)$ stand for the number of factorization patterns of n. Then

$$F(n) = \sum_{\pi \in P_n} \prod_{j=1}^{n} \left[\sum_{\beta \in P_{\pi_j}} 1 \right] = \sum_{\pi \in P_n} \prod_{j=1}^{n} p(\pi_j).$$

This illustrates the recursive approach to computing $N_q(n)$ for any finite field F. However, in case $F = Z_p$, it certainly is not the quickest approach to this problem. The approach in [11] or [9, p. 91-93] based on Möbius inversion is much more efficient. Nevertheless, we hope this simple application conveys to the reader something of the ubiquity and the beauty of partitions of natural numbers. The reader with a further interest in the subject of partitions might consult [1] for more information.

References

1. Andrews, G. E., The theory of partitions, *Encyclopedia of Mathematics and Its Applications* **2**, Addison-Wesley, 1976.
2. Agarwal, A. K., and G. L. Mullen, Partitions with "$d(a)$ copies of a", *J. Combinatorial Theory, Series A* **48** (1988), 120 -135.
3. Bell, E. T., Exponential polynomials, *Annals of Math. II* **35** (1934), 258-277.
4. Biggs, N. L., *Discrete Mathematics*, Clarendon Press, Oxford, 1989.
5. Childs, L., *A Concrete Introduction to Higher Algebra*, Springer-Verlag, 1979.
6. Herstein, I. N., *Topics in Algebra*, 2nd Ed., Xerox, 1975.
7. Hardy, G. H. and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford, 1960.
8. James, G. and A. Kerber, The representation theory of the symmetric group, *Encyclopedia of Mathematics and Its Applications* **16**, Addison-Wesley, 1981.
9. Lidl, R. and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, revised ed., Cambridge University Press, 1994.
10. Pinter, C. C., *A Book of Abstract Algebra*, 2nd ed., McGraw-Hill, 1990.
11. Simmons, G., On the number of irreducible polynomials of degree d over $GF(p)$, *Amer. Math. Monthly* **77** (1970), 743-745.
12. Vella, D., Taylor series of composite functions and combinatorial identities, unpublished (available upon request from the author).

This paper is a portion of Julia Varbalow's senior thesis, written at Skidmore College under the direction of David C. Vella. Ms. Varbalow went on graduate work at the University of Kentucky, while Professor Vella stayed put.