Finite vector spaces and certain lattices

Thomas W. Cusick

106 Diefendorf Hall, Department of Mathematics,
State University of New York at Buffalo, Buffalo, NY 14214-3093
E-mail: cusick@acsu.buffalo.edu

Submitted: January 6, 1998; Accepted: March 18, 1998

Abstract

The Galois number $G_n(q)$ is defined to be the number of subspaces of the n-dimensional vector space over the finite field $GF(q)$. When q is prime, we prove that $G_n(q)$ is equal to the number $L_n(q)$ of n-dimensional mod q lattices, which are defined to be lattices (that is, discrete additive subgroups of n-space) contained in the integer lattice $\mathbf{Z}^n$ and having the property that given any point P in the lattice, all points of $\mathbf{Z}^n$ which are congruent to P mod q are also in the lattice. For each n, we prove that $L_n(q)$ is a multiplicative function of q.

Keywords: Multiplicative function; Lattice; Galois numbers; Vector space; Identities
1991 Mathematical Reviews subject numbers: Primary 05A15 05A19 11A25 11H06
Secondary 05A30 94A60 11T99

1 Introduction

The well known *Gaussian coefficient* (or q-binomial coefficient)

$$\binom{n}{r}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)}$$

is equal to the number of r-dimensional vector subspaces of the n-dimensional vector space $V_n(q)$ over the finite field $GF(q)$. We let $G_n = G_n(q)$ denote the total number of vector subspaces of $V_n(q)$. The numbers G_n were named the *Galois numbers* by Goldman and Rota [4, p. 77].

Goldman and Rota [4] proved the recursion formula

$$G_{n+1} = 2G_n + (q^n-1)G_{n-1} \tag{1}$$

for the Galois numbers.

Nijenhuis, Solow and Wilf [4] gave a different proof of (1) by using the observation that the r-dimensional vector subspaces of $V_n(q)$ are in one-to-one correspondence with the n by n matrices over $GF(q)$ which have rank r and are in reduced row echelon form (rref). Recall that such a matrix is in rref if its last $n-r$ rows are all zeros; in each of the first r rows the first nonzero entry is a 1; the index of the i-th column (called a *pivotal column*) in which one of these r 1's occurs strictly increases as i increases; and each of these r pivotal columns has only a single nonzero entry. We let $E(r,n,q)$ denote the number of n by n matrices with rank r over the field $GF(q)$ which are in rref. Then it was proved in [4] that

$$G_n(q) = \sum_{r=0}^{n} E(r,n,q). \tag{2}$$

The correspondence mentioned above gives

$$E(r,n,q) = \binom{n}{r}_q. \tag{3}$$

For example, $E(r,4,2)$ for $r = 0,1,2,3,4$ is $1, 15, 35, 15$ and 1, respectively.

We shall need the concept of an n-dimensional *mod q lattice*, which is defined to be an n-dimensional lattice contained in the integer lattice $\mathbf{Z}^n$ and having the special property that given any point P in the lattice, all points of $\mathbf{Z}^n$ which are congruent to P mod q are also in the lattice. Later in this paper we shall show how the mod q lattices are connected to the Galois numbers $G_n(q)$. It also turns out that the mod q lattices have an important application in cryptography, which we discuss elsewhere [2]. The set of mod q lattices contains various special subsets which can be used in the design of a novel kind of public-key cryptosystem. This idea originated with Ajtai [1].

2 The multiplicative property

We let $L_m(q)$ denote the number of m-dimensional mod q lattices. Our first goal is to prove that $L_m(q)$ is a multiplicative function, that is, for any positive integers r and s with $\gcd(r, s) = 1$ we have $L_m(rs) = L_m(r)L_m(s)$.

Theorem 1. *The function $L_m(q)$ is multiplicative for each $m = 2, 3, \ldots$.*

Proof. Clearly, every m-dimensional mod q lattice is the solution space of some system

$$A\mathbf{x} \equiv 0 \bmod q, \tag{4}$$

where A is an m by m matrix over the integers mod q. Conversely, the solution space of any system (4) is a mod q lattice. (Note that if $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m$ is the standard basis for $\mathbf{R}^m$, then the m linearly independent vectors $q\mathbf{e}_i$ $(1 \le i \le m)$ are always solutions of (4), so the solution space is always a lattice of dimension m.)

If $\gcd(r, s) = 1$, there is a bijection between the set of m-dimensional mod rs lattices and the set of pairs of m-dimensional lattices made up of one mod r lattice and one mod s lattice. The bijection is defined as follows: Given a mod rs lattice which is the solution space of $A\mathbf{x} \equiv 0 \bmod rs$, we associate with it the pair of lattices which are solution spaces of

$$B\mathbf{x} \equiv 0 \bmod r \text{ and } C\mathbf{x} \equiv 0 \bmod s, \tag{5}$$

where the matrices B and C are defined by

$$A \equiv B \bmod r \text{ and } A \equiv C \bmod s; \tag{6}$$

and conversely, given (5) we define a matrix A by (6).

To prove that this is a bijection, we must first show that different lattice pairs give different mod rs lattices. Given relatively prime integers r and s, by the definition of $L_m(q)$ we can choose two sets of matrices $\{B_i : 1 \le i \le L_m(r)\}$, where B_i is defined over the integers mod r, and $\{C_i : 1 \le i \le L_m(s)\}$, where C_i is defined over the integers mod s, such that every m-dimensional mod r lattice is the solution space of exactly one of the systems $B_i\mathbf{x} \equiv 0 \bmod r,\ 1 \le i \le L_m(r)$, and every m-dimensional mod s lattice is the solution space of exactly one of the systems $C_j\mathbf{x} \equiv 0 \bmod s,\ 1 \le j \le L_m(s)$. Since $\gcd(r, s) = 1$, the theory of linear congruences in one variable shows that each pair of simultaneous congruences

$$A \equiv B_i \bmod r,\ A \equiv C_j \bmod s,\ 1 \le i \le L_m(r),\ 1 \le j \le L_m(s) \tag{7}$$

defines a unique m by m matrix $A = A_{ij}$, say, over the integers mod rs, and these matrices are all different since the pairs B_i, C_j are. We shall show that the solution spaces (which are the mod rs lattices) of the systems

$$A_{ij}\mathbf{x} \equiv 0 \bmod rs,\ 1 \le i \le L_m(r),\ 1 \le j \le L_m(s)$$

are all distinct.

Let A_{IJ} and A_{KL} be any two different matrices chosen from the A_{ij}'s. Then by (7),

$$\{\mathbf{x} \bmod r : A_{IJ}\mathbf{x} \equiv 0 \bmod rs\} = \{\mathbf{x} : B_I\mathbf{x} \equiv 0 \bmod r\}$$

and

$$\{\mathbf{x} \bmod s : A_{IJ}\mathbf{x} \equiv 0 \bmod rs\} = \{\mathbf{x} : C_J\mathbf{x} \equiv 0 \bmod s\};$$

similar equations hold for A_{KL}. Since the pairs B_I, C_J and B_K, C_L are different, we have either

$$\{\mathbf{x} : B_I\mathbf{x} \equiv 0 \bmod r\} \neq \{\mathbf{x} : B_K\mathbf{x} \equiv 0 \bmod r\}$$

or

$$\{\mathbf{x} : C_J\mathbf{x} \equiv 0 \bmod s\} \neq \{\mathbf{x} : C_L\mathbf{x} \equiv 0 \bmod s\},$$

so the solution spaces for A_{IJ} and A_{KL} are different.

Finally we must show that different mod rs lattices give different lattice pairs. This is clear since each congruence $A\mathbf{x} \equiv 0 \bmod rs$ gives a unique pair of congruences (5), where the matrices B and C are defined by (6). □

3 Counting mod q lattices

Our first goal is to prove explicit formulas for the number of m-dimensional mod q lattices, which we denote by $L_m(q)$, when m is small.

Theorem 2. *The numbers $L_2(q)$ and $L_3(q)$ are given by*

$$L_2(q) = \sum_{k_1|q}\sum_{k_2|q} \gcd\left(k_1, \frac{q}{k_2}\right) \tag{8}$$

and

$$L_3(q) = \sum_{k_1|q}\sum_{k_2|q}\sum_{k_3|q} \gcd\left(k_1, \frac{q}{k_3}\right) \gcd\left(k_2, \frac{q}{k_3}\right) \gcd\left(k_1, \frac{q}{k_2}\right). \tag{9}$$

We shall prove formula (8) first. We fix an x_1, x_2 Cartesian coordinate system in $\mathbf{R}^2$. Given any 2-dimensional mod q lattice Λ, we have a basis-free representation for it as follows: The x_1 axis contains infinitely many points of Λ, with a density $1/k_1$, where k_1 is a positive integer which divides q. Every line $x_2 = c$ either contains no points of Λ or contains a shifted copy of the set of lattice points on $x_2 = 0$. If $x_2 = k_2$ is the line $x_2 = c > 0$ which is closest to the x_1 axis and has points of Λ, then k_2 is a divisor of q. A line $x_2 = c$ contains points of Λ if and only if has the form $x_2 = tk_2$ for some integer t. We say that Λ has *jump* k_2 (in the x_2 direction). If we let $C_2(\Lambda)$ denote the 2-dimensional volume of a fundamental cell of Λ, then we have $C_2(\Lambda) = k_1k_2$.

To count the 2-dimensional mod q lattices which have given values of k_1 and k_2, it suffices to count the number of distinct 1-dimensional sublattices on $x_2 = k_2$ which give a mod q lattice. We define the *shift* s, where s is an integer such that $0 \le s < k_1$, to be the amount by which the 1-dimensional sublattice on $x_2 = k$ is shifted with respect to the 1-dimensional sublattice on $x_2 = 0$. In order to give a mod q lattice, the shift s must give a 1-dimensional sublattice on $x_2 = q$ which is an unshifted copy of the same sublattice on $x_2 = 0$. The sublattice on $x_2 = q$ is shifted from the one on $x_2 = 0$ by qs/k_2, so the shift s gives a mod q lattice if and only if

$$k_1 \text{ divides } qs/k_2. \tag{10}$$

Clearly (10) holds for given k_1 and k_2 if and only if $k_1k_2/\gcd(k_1k_2, q) = D$, say, divides s. Thus there are $k_1/D = \gcd(k_1, q/k_2)$ allowable values of s in the range $0 \le s < k_1$. This proves (8).

Now we prove formula (9). Each 3-dimensional mod q lattice Λ is made up of a 2-dimensional mod q sublattice in the x_1, x_2 plane, which we denote by P_0, and shifted copies of this sublattice in each of various planes P_i (i nonzero integer) which are equally spaced parallel to P_0. As before, we let $1/k_1$ denote the density of the points of Λ on the x_1 axis and we let k_2 denote the jump in the x_2 direction for the sublattice in P_0 (and so for Λ). The plane P_1 nearest to P_0 is at a distance k_3, where k_3 is a divisor of q. We say that Λ has jump k_3 in the x_3 direction. If we let $C_3(\Lambda)$ denote the 3-dimensional volume of a fundamental cell of Λ, then we have $C_3(\Lambda) = k_1k_2k_3$.

To count the 3-dimensional mod q lattices with given k_1, k_2 and k_3, for each 2-dimensional mod q sublattice on P_0 we count the number of distinct 2-dimensional sublattices in $x_3 = k_3$ (i.e., the plane P_1) which give a mod q lattice. We let s denote the shift for the 1-dimensional sublattices in P_0, as before, and we define the (vector) shift $\mathbf{s} = (s_1, s_2)$, where $0 \le s_i < k_i$ ($i = 1, 2$), to be the amount by which $\mathbf{0}$ in P_0 is moved when we go to the sublattice in P_1. The shift $\mathbf{s}$ gives a mod q lattice if and only if

$$k_1 \text{ divides } qs_1/k_3 \text{ and } k_2 \text{ divides } qs_2/k_3, \tag{11}$$

that is, if and only if the orthogonal projection of $(q/k_3)(s_1, s_2, k_3)$ into the plane P_0 is a lattice point. Now (11) holds for given k_1, k_2 and k_3 if and only if $k_ik_3/\gcd(k_ik_3, q) = D_i$, say, divides s_i ($i = 1, 2$). Thus there are $k_i/D_i = \gcd(k_i, q/k_3)$ allowable values of s_i in the range $0 \le s_i < k_i$. This proves (9).

It is possible to extend the formula in Theorem 2 to the case of general m, but complicated m-fold sums are involved. Since we do not need this result, we do not give it here.

A multiplicative function is completely determined by its values at prime powers, so it is of interest to examine $L_m(p^a)$ for prime p. Direct calculation using (8) gives

$$L_2(p^a) = \sum_{i=0}^{a} (1 + 2i)p^{a-i} = \frac{(p + 1)p^{a+1} - (2a + 3)p + 2a + 1}{(p - 1)^2}.$$

Computer calculations using (9) give Table 1, which shows the expansion of $L_3(p^a)$ in powers of p for small a. There does not seem to be any nice explicit formula for $L_3(p^a)$, though various properties of the coefficients in the table can be deduced. Table 2 gives some values for $L_2(q)$ and $L_3(q)$.

$a, j \rightarrow$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	4	2	2												
2	7	6	6	5	3										
3	10	10	12	10	10	8	4								
4	13	14	18	17	18	14	15	11	5						
5	16	18	24	24	28	22	24	20	20	14	6				
6	19	22	30	31	38	32	35	30	30	27	25	17	7		
7	22	26	36	38	48	42	48	42	42	38	38	34	30	20	8

Table 1: Coefficients of p^j in the expansion of $L_3(p^a)$, $a \leq 7$.

	2	3	4	5	7	8	9	11	13	16	17	19	23
$L_2(q)$	5	6	15	8	10	37	23	14	16	83	20	22	26
$L_3(q)$	16	28	131	64	116	830	457	268	368	4633	616	1016	1108

Table 2: Values of $L_2(q)$ and $L_3(q)$ for small prime powers q.

4 The connection with Galois numbers

Because of (2), our next theorem shows that $L_m(q) = G_m(q)$ whenever q is a prime.

Theorem 3. *For any prime q, we have*

$$L_m(q) = \sum_{r=0}^{m} E(r, m, q).$$

Proof. We have already seen that every m-dimensional mod q lattice is the solution space of some system (4), where A is an m by m matrix over the integers mod q. Conversely, the solution space of any system (4) is an m-dimensional mod q lattice. Since q is prime, the mod q lattices are thus in one-to-one correspondence with the m by m reduced row echelon forms of matrices over $GF(q)$ and we have the desired equation. □

Because of (3), it is easy to compute $E(r, m, q)$ for given values of r, m, q.

If q is not prime, the first two sentences in the proof of Theorem 3 are still true, so the one-to-one correspondence between the mod q lattices and solution spaces of systems (4) is still valid. What is lost is the link with matrices over a field which are in reduced row echelon form (rref). Thus this paper shows that there are two different natural extensions of the Galois numbers $G_n(q)$, q prime. One extension leads to the Galois numbers $G_n(q)$ for arbitrary positive integers q, as given in [4]. In that paper a formal definition of a rref matrix over a set of q symbols is given and finite fields play no role. For each n, the numbers $G_n(q)$ are fixed polynomials in q, and the recursion (1) holds as a polynomial identity. The other extension leads to the multiplicative functions $L_n(q)$ in this paper. If q is not prime, then $L_n(q)$ is not a polynomial in q and the analog of (1) does not hold.

References

[1] Miklos Ajtai, Generating hard instances of lattice problems, in: *Proc. 28th ACM Symposium on the Theory of Computing, 1996*, pp. 99-108.

[2] Thomas W. Cusick, The Ajtai random class of lattices, to appear.

[3] Jay Goldman and Gian-Carlo Rota, The number of subspaces of a vector space, in: *Recent Progress in Combinatorics*, ed. W. T. Tutte (Academic Press, 1969), pp. 75-83.

[4] Albert Nijenhuis, Anita E. Solow and Herbert S. Wilf, Bijective methods in the theory of finite vector spaces, *J. Combin. Theory (A)* 37 (1984), 80-84.