

# Factorial Factors

John R. Silvester

An easy counting argument with vectors in section 1 gives the well known result that  $n!$  is a factor of  $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$ , whenever  $q$  is a prime power. In section 2, we show that the result is true for every integer  $q$ , by a proof that involves counting, for each prime  $p$ , how many times  $p$  divides  $n!$  and how many times it divides  $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$ , and comparing. As a spin-off, in section 3, we obtain an easy way of answering the old chestnut about how many zeros there are at the end of  $n!$ .

## 1 Counting bases of a vector space

How do we set about finding a basis for a vector space? For example, if we want a basis  $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$  for  $\mathbb{R}^3$ , we choose the first element  $\mathbf{v}_1$  to be any vector in  $\mathbb{R}^3$  *except* the zero vector; that is, we avoid the zero-dimensional subspace. Then, for the second element  $\mathbf{v}_2$  we can choose any vector not linearly dependent on  $\mathbf{v}_1$ ; that is, we avoid the 1-dimensional subspace spanned by  $\mathbf{v}_1$ . For the final element  $\mathbf{v}_3$  we can now choose any vector not linearly dependent on  $\mathbf{v}_1$  and  $\mathbf{v}_2$ ; that is, we avoid the 2-dimensional subspace spanned by  $\mathbf{v}_1$  and  $\mathbf{v}_2$ .

Let's do this using a different field of scalars: we'll use the field  $\mathbb{F}$ , which we are going to suppose is *finite*: specifically, suppose  $|\mathbb{F}| = q$ . (For example, we might choose  $\mathbb{F} = \mathbb{Z}_p$ , integers modulo a prime number  $p$ . In that case we would have  $q = p$ .) Over such a field, an  $r$ -dimensional space (or subspace of a space) must be isomorphic to  $\mathbb{F}^r$ , and so will contain  $q^r$  elements.

So, to choose a basis  $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$  of  $\mathbb{F}^3$ , we have a choice of  $q^3 - 1$  vectors for  $\mathbf{v}_1$ , a choice of  $q^3 - q$  vectors for  $\mathbf{v}_2$ , and a choice of  $q^3 - q^2$  vectors for  $\mathbf{v}_3$ . Thus the number of different bases is

$$(q^3 - 1)(q^3 - q)(q^3 - q^2).$$

More generally, the number of different bases of  $\mathbb{F}^n$  is

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}),$$

since there are  $q^n$  vectors altogether, and at the  $(r + 1)^{\text{th}}$  step we are trying to avoid the  $q^r$  vectors in the  $r$ -dimensional subspace spanned by the vectors already chosen.

Of course, if we write the elements of a basis in a different order, we get another basis, and this means that the different bases fall into equivalence classes of  $n!$  bases each, under

the action of permuting the elements. (Remember that the elements of a basis must be distinct.) As is well known, it follows that

$$\frac{(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})}{n!}$$

is an integer, being the number of equivalence classes, that is, the number of *unordered* bases of  $\mathbb{F}^n$ .

Thus we have proved that

$$n! \mid (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}),$$

where the symbol “ $\mid$ ” means “divides”, or “is a factor of”.

For those who like group theory, an alternative version of the argument might run thus: the general linear group  $GL_n(\mathbb{F})$ , of all invertible  $n \times n$  matrices over  $\mathbb{F}$ , has order

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}),$$

the successive brackets being the number of choices for successive rows of an invertible matrix. The permutation matrices (obtained by permuting the rows, or columns, of the identity matrix) form a subgroup of this, of order  $n!$ , and the result follows by Lagrange’s theorem.

Now, if  $q = |\mathbb{F}|$ , where  $\mathbb{F}$  is a field, then  $\mathbb{F}$  contains a minimal subfield isomorphic to  $\mathbb{Z}_p$ , where  $p$  is a prime number, the *characteristic* of  $\mathbb{F}$ . Here  $p$  is the additive order of 1 in  $\mathbb{F}$ , necessarily prime, and  $\mathbb{Z}_p$  is the *prime subfield* of  $\mathbb{F}$ . But this means that  $\mathbb{F}$  can be regarded as a vector space over  $\mathbb{Z}_p$ . Since it is finite, it is certainly finite-dimensional; and if its dimension is  $r$  then  $\mathbb{F} \cong \mathbb{Z}_p^r$  (as  $\mathbb{Z}_p$ -spaces), and therefore  $q = p^r$ . So the order of a finite field is a prime power; and in fact for every prime power there is, up to isomorphism, precisely one finite field of that order. (See [1], Theorem 16.4.)

To recap, we have proved that

$$n! \mid (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}), \tag{1}$$

but we now see that the above proof will only work if  $q$  is a prime power.

## 2 The general case

In fact, (1) is true for every  $q$ ; this seems to be not so well known, and the proof that follows is a bit fiddly. What we shall do is calculate, for *every* prime  $p$ , how many times  $p$  divides each side of (1), and compare.

First, the LHS of (1). How many times does  $p$  divide  $n!$  ?

$p$  divides *once* into each of  $p, 2p, 3p, \dots$ ;  
a *second* time into each of  $p^2, 2p^2, 3p^2, \dots$ ;  
a *third* time into each of  $p^3, 2p^3, 3p^3, \dots$ ;

and so on. The number of multiples of  $m$  that are less than or equal to  $n$  is the integer part of  $n/m$ , which we denote  $[n/m]$ . We conclude:  $n!$  is divisible by  $p^r$  (and not by  $p^{r+1}$ ), where

$$r = \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \left[ \frac{n}{p^3} \right] + \dots \quad (2)$$

(This makes sense, as all but a finite number of terms on the right are zero.)

Note that, from (2),

$$r < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \dots$$

so that, summing the geometric progression, we have

$$r < \frac{n}{p-1}. \quad (3)$$

Now for the RHS of (1). Note that

$$\begin{aligned} & (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}) \\ &= q^s (q^n - 1)(q^{n-1} - 1)(q^{n-2} - 1) \dots (q - 1) \end{aligned} \quad (4)$$

where

$$s = 0 + 1 + 2 + \dots + (n-1) = \frac{n(n-1)}{2}.$$

Since  $p$  is prime, either  $p \mid q$  or else  $p$  and  $q$  are coprime.

CASE 1. Suppose  $p \mid q$ . Here we need to show that  $r \leq s$ , that is,

$$r \leq \frac{n(n-1)}{2}. \quad (5)$$

If  $n = p = 2$ , then  $r = [n/p] = 1$  and also  $\frac{n(n-1)}{2} = 1$ , so (5) follows. On the other hand, if  $n > 2$  or  $p > 2$  (or both) then  $n \geq 3$  or  $p \geq 3$  (or both), so

$$2 \leq (n-1)(p-1),$$

whence

$$\frac{n}{p-1} \leq \frac{n(n-1)}{2}.$$

But (3) says  $r < \frac{n}{p-1}$ , so (5) follows again, and this completes case 1.

CASE 2. Suppose  $p$  and  $q$  are coprime. Then we know that  $p$  divides  $q^{p-1} - 1$ , by Fermat's little theorem; and likewise  $p$  divides  $q^{2(p-1)} - 1$ ,  $q^{3(p-1)} - 1$ , and so on. The number of terms  $(q^k - 1)$  divisible by  $p$  on the RHS of (4) is thus at least  $\left\lfloor \frac{n}{p-1} \right\rfloor$ . But (3) says  $r < \frac{n}{p-1}$ , and since  $r$  is an integer, we must in fact have  $r \leq \left\lfloor \frac{n}{p-1} \right\rfloor$ . This completes case 2 and so finishes the proof: for all  $n$  and  $q$ ,

$$n! \mid (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}).$$

One feels there ought to be a counting argument in the general case: surely the brackets must represent successive choices of  $n$  objects, and the divisibility by  $n!$  must follow from some argument about choosing the same objects in a different order? The author has been unable to find any such argument other than in the special case given in section 1, and would be glad to hear of any suggestions from readers.

### 3 Counting noughts

Here is a nice application of equation (2), above. A recent edition of *Mathematical Pie* (No. 156, Summer 2002) contained the following problem, called *Counting Noughts*:

The symbol  $50!$  represents the value of  $1 \times 2 \times 3 \times 4 \times \dots \times 49 \times 50$ . If we were to calculate the actual value, how many zeros would the final answer have?

The accompanying notes told us that there are "12 noughts in all". But, courtesy of *Maple*,  $50!$  is equal to

$$30414093201713378043612608166064768844377641568960512000000000000$$

and any reader who cares to count will find that there are 19 noughts here. Of course, the intention of the problem was to ask for the number of zeros at the *end* of  $50!$ , that is, the number of times 10 divides  $50!$ . Since  $10 = 2 \times 5$  and  $2 < 5$ , a glance at (2) tells us we just need to know how many times 5 divides  $50!$ , as 2 is bound to divide it *more* times. So from (2), the answer to the problem *is* now 12, since

$$\left\lfloor \frac{50}{5} \right\rfloor + \left\lfloor \frac{50}{25} \right\rfloor = 10 + 2 = 12,$$

other terms in (2) being zero in this case. If instead we ask for the number of zeros at the end of  $1066!$ , the answer is

$$\left\lfloor \frac{1066}{5} \right\rfloor + \left\lfloor \frac{1066}{25} \right\rfloor + \left\lfloor \frac{1066}{125} \right\rfloor + \left\lfloor \frac{1066}{625} \right\rfloor = 213 + 42 + 8 + 1 = 264.$$

Note that successive terms here can be obtained most easily by repeated division by 5, throwing away any remainder:  $[1066/5] = 213$ ,  $[213/5] = 42$ , and so on; and generally, if  $a_k = [n/p^k]$ , then  $a_{k+1} = [a_k/p]$ .

#### REFERENCE

[1] Ian Stewart, *Galois Theory* (2nd edition), Chapman and Hall (1989).

*Department of Mathematics*

*King's College*

*Strand*

*London WC2R 2LS*

*(Email: jrs@kcl.ac.uk)*

*27 July 2002*

*(revised 29 October 2003)*