FACTORIAL FACTORS

John R. Silvester
Department of Mathematics
King's College London

Preliminaries: the product of n successive positive integers is divisible by $n!$. For if we choose n elements from a set of order m, where $m \geq n$, we may choose the first element m ways, the second $m-1$ ways, and so on, giving

$$m(m-1)(m-2)\dots(m-n+1)$$

possible (ordered) choices. If we make one choice equivalent to another when its elements are a permutation of the elements of the other, we separate the set of choices into equivalence classes of $n!$ elements each, so that

$$\frac{m(m-1)(m-2)\dots(m-n+1)}{n!}$$

is the number of possible (unordered) choices of n objects from m. This is also written $\binom{m}{n}$ or ${}^mC_n$, and is the coefficient of x^n in the (binomial) expansion of $(1+x)^m$.

Here is a hoary old problem that reappears every Christmas:

According to the song, how many presents did my true love send to me?

(N.B. A partridge in a pear tree counts as *one* present.)

Let (r, s, t) denote the r^{th} present of type s received on the t^{th} day of Christmas.

So, for example, $(3, 5, 8)$ stands for the 3^{rd} of the 5 gold rings received on the 8^{th} day.

We must count all integer triples (r, s, t) with

$$1 \le r \le s \le t \le 12,$$

or (equivalently)

$$1 \le r < s' < t'' \le 14$$

(where s' means $s+1$, and t'' means $t+2$), and so the answer is

$$\binom{14}{3} = \frac{14 \times 13 \times 12}{3!} = 364.$$

A simpler problem: evaluate $1 + 2 + 3 + \ldots + n$.

Solution (by counting): write it as

$$(1) + (1 + 1) + (1 + 1 + 1) + \ldots + (1 + 1 + \ldots + 1)$$

where the last bracket contains n 1's. Then let (r, s) denote the r^{th} 1 in the s^{th} bracket. We must count all integer pairs (r, s) with

$$1 \leq r \leq s \leq n,$$

or (equivalently)

$$1 \leq r < s' \leq n + 1,$$

and so the answer is

$$\binom{n+1}{2}.$$

Thus

$$\sum_{r=1}^{n} r = \binom{n+1}{2}$$

or, more suggestively,

$$\sum_{r=1}^{n} \binom{r}{1} = \binom{n+1}{2}, \quad \text{or} \quad \sum_{r=0}^{n} \binom{r+1}{1} = \binom{n+2}{2}.$$

In the partridge-in-a-pear-tree problem, the number of presents received on day s was $1+2+\ldots+s = \binom{s+1}{2}$, so the solution amounted to saying that

$$\sum_{s=1}^{12} \binom{s+1}{2} = \binom{14}{3}, \quad \text{or} \quad \sum_{s=0}^{11} \binom{s+2}{2} = \binom{11+3}{3}.$$

In fact, for any n,

$$\sum_{s=0}^{n} \binom{s+2}{2} = \binom{n+3}{3},$$

and more generally (as we shall prove next)

$$\sum_{s=0}^{n} \binom{s+k}{k} = \binom{n+k+1}{k+1}.$$

Proof: note first that $\binom{s+k}{k}$ is the number of ways of choosing integers a_1, a_2, . . . , a_k with $1 \le a_1 < a_2 < \ldots < a_k \le s+k$, or

$$1 \le a_1 < a_2 < \ldots < a_k < s+k+1.$$

Put $a_{k+1} = s+k+1$, and then as s runs from 0 to n, altogether we get the number of ways of choosing a_1, a_2, . . . , a_k, a_{k+1}, with

$$1 \le a_1 < a_2 < \ldots < a_k < a_{k+1} \le n+k+1,$$

and this is just $\binom{n+k+1}{k+1}$, as required.

Alternative proof: we have

$$1 + y + y^2 + \ldots + y^{n+k} = \frac{y^{n+k+1} - 1}{y - 1},$$

and on putting $y = 1 + x$ this becomes

$$1 + (1+x) + (1+x)^2 + \ldots + (1+x)^{n+k} = \frac{(1+x)^{n+k+1} - 1}{x}.$$

The result follows on comparing coefficients of x^k on each side.

More applications: note that

$$s^2 = \binom{s}{2} + \binom{s+1}{2}. \qquad (\star)$$

This is pretty obvious anyway; but can be seen by counting.

We must count all (a, b) with $1 \leq a \leq s$ and $1 \leq b \leq s$.

For each such pair (a, b) we have

$$a < b \quad \text{or else} \quad b \leq a,$$

so we have

$$1 \leq a < b \leq s \quad \text{or else} \quad 1 \leq b < a' \leq s + 1,$$

which give the first and second terms of $(\star)$, respectively.

From $(\star)$ we have

$$\begin{aligned}\sum_{s=1}^{n} s^2 &= \binom{n+1}{3} + \binom{n+2}{3} \\ &= \frac{(n+1)n(n-1)}{6} + \frac{(n+2)(n+1)n}{6} \\ &= \frac{n(n+1)\Big((n-1)+(n+2)\Big)}{6} \\ &= \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

Alternatively,

$$\begin{aligned} 4\sum_{s=1}^{n} s^2 &= \sum_{s=1}^{n} (2s)^2 \\ &= \sum_{s=1}^{n} \left(\binom{2s}{2} + \binom{2s+1}{2} \right) \\ &= \sum_{s=2}^{2n+1} \binom{s}{2} \\ &= \binom{2n+2}{3} \\ &= \frac{(2n+2)(2n+1)(2n)}{6}, \end{aligned}$$

so now divide each side by 4.

Now for the cubes. s^3 is the number of ways of choosing (p, q, r) with $1 \le p \le s$, $1 \le q \le s$, and $1 \le r \le s$.

Case 1: $|\{p, q, r\}| = 3$, that is, p, q, r are distinct. This now subdivides into $3! = 6$ cases according to the relative sizes of p, q, and r: for example, one case is $1 \le p < q < r \le s$, and the total count for case 1 is $6\binom{s}{3}$.

Case 2: $|\{p, q, r\}| = 2$, so that two of p, q, r are equal, but different from the third. We can choose the two that are equal in 3 ways, and then the third is either greater or less than the others, so again there are 6 cases; for example, one is $1 \le p = q < r \le s$, and the total count for case 2 is $6\binom{s}{2}$.

Case 3: $|\{p, q, r\}| = 1$, or $p = q = r$, so that $1 \le p = q = r \le s$, and the count here is just s, or $\binom{s}{1}$.

So

$$s^3 = 6\binom{s}{3} + 6\binom{s}{2} + \binom{s}{1},$$

and therefore

$$\sum_{s=1}^{n} s^3 = 6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2}.$$

We shall show, *by counting*, that this is the same as

$$\left(\sum_{s=1}^{n} s\right)^2,$$

so that its value is

$$\frac{n^2(n+1)^2}{4}.$$

Recall that $1 + 2 + \ldots + n$ is the number of pairs (a, b) with $1 \le a < b \le n + 1$. So $(1 + 2 + \ldots + n)^2$ is the number of 4-tuples (a, b, c, d) with $1 \le a < b \le n + 1$ and $1 \le c < d \le n + 1$.

Case 1: $|\{a, b, c, d\}| = 4$. There are 6 subcases:

$$
\begin{aligned}
&1 \le a < b < c < d \le n + 1, \qquad && 1 \le a < c < b < d \le n + 1,\\
&1 \le a < c < d < b \le n + 1, \qquad && 1 \le c < a < b < d \le n + 1,\\
&1 \le c < a < d < b \le n + 1, \qquad && 1 \le c < d < a < b \le n + 1.
\end{aligned}
$$

So the total count here is

$$6\binom{n+1}{4}.$$

Case 2: $|\{a,b,c,d\}| = 3$. Again, there are 6 subcases:

$$\begin{array}{ll} 1 \leq a = c < b < d \leq n+1, & 1 \leq a = c < d < b \leq n+1, \\ 1 \leq c < a = d < b \leq n+1, & 1 \leq a < b = c < d \leq n+1, \\ 1 \leq a < c < b = d \leq n+1, & 1 \leq c < a < b = d \leq n+1. \end{array}$$

So the total count here is

$$6\binom{n+1}{3}.$$

Case 3: $|\{a,b,c,d\}| = 2$. Here $1 \leq a = c < b = d \leq n+1$, so the count for this case is

$$\binom{n+1}{2}.$$

To sum up (!),

$$\begin{aligned}\sum_{s=1}^{n} s^3 &= 6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2} \\ &= \left(\sum_{s=1}^{n} s\right)^2 \\ &= \binom{n+1}{2}^2.\end{aligned}$$

The reader is invited to find an alternative proof by showing that

$$\binom{n+1}{2}^2 - \binom{n+1}{2} = 6\binom{n+2}{4}$$

and that

$$\binom{n+2}{4} = \binom{n+1}{4} + \binom{n+1}{3}.$$

Do either of these formulae generalize?

Yet again, we know

$$s^2 = \binom{s}{2} + \binom{s+1}{2},$$

and you can easily obtain (by counting!) that

$$s^3 = \binom{s}{3} + 4\binom{s+1}{3} + \binom{s+2}{3}.$$

Exercise: obtain coefficients a_{ij} such that

$$s^r = a_{r1}\binom{s}{r} + a_{r2}\binom{s+1}{r} + \ldots + a_{rr}\binom{s+r-1}{r}$$

for the next few values of r, and investigate the properties of the Pascal-like triangle of numbers a_{ij}.

You should get:

1

1 1

1 4 1

1 11 11 1

1 26 66 26 1

1 57 302 302 57 1

1 120 1191 2416 1191 120 1

1 247 4293 15619 15619 4293 247 1

... ...

By courtesy of the On-Line Encyclopedia of Integer Sequences (www.research.att.com/~njas/sequences/) I now know that the above numbers are the *Eulerian numbers* and the triangle is known as *Euler's number triangle*. Given a permutation $\rho : i \mapsto \rho_i$ of $\{1, 2, \ldots, n\}$, we write the list of images $\{\rho_1, \rho_2, \ldots, \rho_n\}$; in this list, an *ascent* is a pair of adjacent elements that are in descending order. For example, if $n = 6$ and ρ sends $\{1, 2, 3, 4, 5, 6\}$ to $\{2, 4, 5, 3, 1, 6\}$ respectively, then ρ has two ascents, $\{5, 3\}$ and $\{3, 1\}$.

The Eulerian number $\left\langle {n \atop k} \right\rangle$, where $0 \leq k < n$, is defined to be the number of permutations of $\{1, 2, \ldots, n\}$ having exactly k ascents.

Immediate observations: for $0 \leq k \leq n-1$, $\left\langle {n \atop k} \right\rangle$ is a positive integer, with $\left\langle {n \atop 0} \right\rangle = 1$ and $\left\langle {n \atop n-1} \right\rangle = 1$; and obviously

$$\left\langle {n \atop 0} \right\rangle + \left\langle {n \atop 1} \right\rangle + \ldots + \left\langle {n \atop n-1} \right\rangle = n!.$$

Next, $\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n-1-k} \right\rangle$, by observing that, if ρ is paired with ρ', where $\rho'_i = n+1-\rho_i$, all i, then the number of ascents in ρ plus the number of ascents in ρ' is $n-1$. Also the relation

$$\left\langle {n \atop k} \right\rangle = (n-k) \left\langle {n-1 \atop k-1} \right\rangle + (k+1) \left\langle {n-1 \atop k} \right\rangle$$

comes from observing that if n is inserted into a permutation of $1, 2, \ldots, n-1$ to produce a permutation of $1, 2, \ldots, n$, then it can be inserted in any of n places, and the number of ascents either stays the same or goes up by 1.

Now for s^r. We have that s^r is equal to the number of ways of choosing $n_1, n_2, \ldots, n_r$ with $1 \leq n_i \leq s$, all i. For each such choice, rearrange the n_i in increasing order; this is unambiguous for distinct values, but where two or more n_i have the *same* value, arrange them so that their *subscripts* are in *decreasing* order. Let the new order be $n_{\rho_1}, n_{\rho_2}, \ldots, n_{\rho_r}$, which defines a unique permutation ρ.

For example, if $s \geq 5$ and $r = 6$, and $n_1 = 4$, $n_2 = 1$, $n_3 = 4$, $n_4 = 3$, $n_5 = 4$ and $n_6 = 5$, then we have the multiple inequality

$$n_2 < n_4 < n_5 \leq n_3 \leq n_1 < n_6,$$

and ρ sends $1, 2, 3, 4, 5, 6$ to $2, 4, 5, 3, 1, 6$ respectively. If instead we had written $n_1 = 5$ and $n_6 = 6$, we would have obtained the stronger condition

$$n_2 < n_4 < n_5 \leq n_3 < n_1 < n_6.$$

Each choice of $n_1, n_2, \ldots, n_r$ thus gives rise to exactly one permutation ρ. The corresponding multiple inequality involves $1 \le n_{\rho_1}$, $n_{\rho_2}, \ldots, n_{\rho_r} \le s$ in that order; if we now insert into this list "$\le$" at each ascent of ρ, and "$<$" elsewhere, then the condition obtained (or maybe a stronger one) is satisfied by our chosen n_i.

The number of ways of solving this multiple inequality, if there are exactly k weak inequalities, is $\binom{s+k}{r}$, and so if we lump together the permutations having the same number of ascents, we obtain

$$s^r = \left\langle {r \atop 0} \right\rangle \binom{s}{r} + \left\langle {r \atop 1} \right\rangle \binom{s+1}{r} + \ldots + \left\langle {r \atop r-1} \right\rangle \binom{s+r-1}{r}.$$

This is the equation

$$s^r = a_{r1}\binom{s}{r} + a_{r2}\binom{s+1}{r} + \ldots + a_{rr}\binom{s+r-1}{r}$$

on page 19, with $a_{rk} = \left\langle {r \atop k-1} \right\rangle$.

Here is a different sort of counting argument. 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.

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 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 $\mathbf{v}_2$.

Now 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

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

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 some r-dimensional subspace.

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. It follows that

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

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

Thus we have proved that

$$n! \,\Big|\, (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}).$$

Alternative posh argument: the general linear group $\mathrm{GL}_n(\mathbb{F})$, 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 $\mathbb{F}$. (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.

To recap, we have proved that

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

but we now see that our proof will not work if q is not a prime power.

In fact, $(\star)$ true for every q, though the proof is a bit fiddly. What we shall do is calculate, for *every* prime p, how many times p divides each side of $(\star)$, and compare.

How many times does p divide $n!$?

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

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

$$r = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

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

Note that

$$r < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots = \frac{n}{p}\left(1 - \frac{1}{p}\right)^{-1} = \frac{n}{p-1}.$$

Next, note that

$$\begin{aligned} & (q^n - 1)(q^n - q)(q^n - q^2)\ldots(q^n - q^{n-1}) \\ = \; & q^s(q^n - 1)(q^{n-1} - 1)(q^{n-2} - 1)\ldots(q - 1) \end{aligned}$$

where

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

Since p is prime, either $p \Big| q$ or else p and q are coprime. In the first case, we need to show that

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

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

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

whence

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

and the result follows, since, as we have already shown, $r < \dfrac{n}{p-1}$.

In the other case, when p and q are coprime, we know that p divides $q^{p-1}-1$, by Fermat's little theorem; and likewise it divides $q^{2(p-1)}-1$, $q^{3(p-1)}-1$, and so on. The number of terms (q^s-1) divisible by p on the RHS of $(\star)$ is thus at least $\left[\dfrac{n}{p-1}\right]$. But we know $r \leq \dfrac{n}{p-1}$, and since r is an integer, we must have $r \leq \left[\dfrac{n}{p-1}\right]$. This finishes the proof: in all cases,

$$n! \;\Big|\; (q^n-1)(q^n-q)(q^n-q^2)\ldots(q^n-q^{n-1}).$$

Suppose we want to combine n elements of some set under a non-associative binary operation. (So $n \geq 2$.) How many ways can we do this, i.e., how many ways can we put in the brackets?

For example, if $n = 3$, the answer is 2, for we can write

$$a(bc) \quad \text{or} \quad (ab)c.$$

Again, if $n = 4$, the answer is 5, for we can write

$$a(b(cd)), \quad a((bc)d), \quad (ab)(cd), \quad (a(bc))d, \quad \text{or} \quad ((ab)c)d.$$

Here is a neat way of getting a formula for the answer, for n symbols. In elementary group theory, the "product" ab, or (ab), is often written using some special symbol such as $\star$, so we might write $a \star b$, to emphasize that this is not (necessarily) ordinary multiplication. We are going to do this, but perversely we shall write it as $\star ab$, not $a \star b$. In this notation, we don't need any brackets! For example, $(ab)c$ is written $\star\star abc$, and $a(bc)$ is written $\star a \star bc$.

To reverse the process, replace each $\star$ by a LH bracket, and you then find there is a unique way of inserting RH brackets to make the answer make sense. For instance,

$$\star \star a\ b \star c\ d \to ((ab(cd \to ((ab(cd) \to ((ab)(cd) \to ((ab)(cd)).$$

The symbols a, b, c, $\ldots$ are just place-holders, so we shall write them *all* as a. A particular way of bracketing a product of n elements can now be represented by a string of $2n-1$ symbols, n a's and $n-1$ $\star$'s.

Not every such string is legal, i.e., makes sense: for example, when $n=2$ the possible strings are

$$\star aa, \quad a \star a, \quad \text{and} \quad aa\star,$$

but only the first of these is legal. However, we make the crucial observation that a suitable (and unique) cyclic permutation of each of the illegal strings will legalize them.

We prove this for general n by induction. We just did the first case, $n = 2$. For larger n, we claim that some cyclic permutation of any given string will contain the sub-string $\star aa$.

Since we have more a's than $\star$'s in our given string, some cyclic permutation of the string (possibly trivial) will bring two or more a's together. However many successive a's occur, they must be preceded by a $\star$ (in the cyclic ordering), so that a cyclic permutation (possibly trivial) will produce the sequence $\star aa$.

We now replace $\star aa$ by a, and this reduces us to the case of $n-1$ a's and $n-2$ $\star$'s, so the result follows by induction.

Here is a worked example with $n = 5$:

$$
\begin{array}{rcccccccccc}
 & a & \star & a & \star & a & a & \star & \star & a & \\
\cline{5-7}
 & a & \star & a & & a & & \star & \star & a & \\
\cline{3-6}
 & a & & a & & & & \star & \star & a & \\
\text{Cycle:} & & & a & & & & \star & \star & a & a \\
\cline{9-11}
 & & & a & & & & \star & & a & \\
\text{Cycle again:} & & & & & & & \star & & a & a \\
\cline{8-11}
 & & & & & & & & & a &
\end{array}
$$

So we *should* have started three from the end:

$$
\begin{array}{rccccccccc}
 & \star & \star & a & a & \star & a & \star & a & a \\
\text{which represents} & (& (& a & a) & (& a & (& a & a))).
\end{array}
$$

We have shown that the number of ways of bracketing a product of n elements is the number of cyclic orderings of $2n-1$ symbols, of which n are the same and the remaining $n-1$ are the same. This is

$$\frac{(2n-2)!}{n!(n-1)!},$$

which we'll denote by $f(n)$. Here are the first few values:

n :	2	3	4	5	6	7	8	9	10
$f(n)$:	1	2	5	14	42	132	429	1430	4862