40. [*HM46*] Study the class of replicative functions; determine all replicative functions of a special type. For example, is the function in (a) of exercise 39 the only continuous replicative function? It may be interesting to study also the more general class of functions for which

$$f(x)+f\left(x+\frac{1}{n}\right)+\cdots+f\left(x+\frac{n-1}{n}\right)=a_nf(nx)+b_n.$$

Here a_n and b_n are numbers that depend on n but not on x. Derivatives and (if $b_n=0$) integrals of these functions are of the same type. If we require that $b_n=0$, we have, for example, the Bernoulli polynomials, the trigonometric functions $\cot\pi x$ and $\csc^2\pi x$, as well as Hurwitz's generalized zeta function $\zeta(s,x)=\sum_{k\ge0}1/(k+x)^s$ for fixed s. With $b_n\ne0$ we have still other well-known functions, such as the psi function.

41. [*M23*] Let a_1, a_2, a_3, $\ldots$ be the sequence 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, $\ldots$; find an expression for a_n in terms of n, using the floor and/or ceiling function.

42. [*M24*] (a) Prove that

$$\sum_{k=1}^{n}a_k=na_n-\sum_{k=1}^{n-1}k(a_{k+1}-a_k),\qquad\text{if } n>0.$$

(b) The preceding formula is useful for evaluating certain sums involving the floor function. Prove that, if b is an integer ≥2,

$$\sum_{k=1}^{n}\lfloor\log_b k\rfloor=(n+1)\lfloor\log_b n\rfloor-(b^{\lfloor\log_b n\rfloor+1}-b)/(b-1).$$

43. [*M23*] Evaluate $\sum_{k=1}^{n}\lfloor\sqrt{k}\,\rfloor$.

44. [*M24*] Show that $\sum_{k\ge0}\sum_{1\le j<b}\lfloor(n+jb^k)/b^{k+1}\rfloor=n$, if b and n are integers, $n\ge0$, and $b\ge2$. What is the value of this sum when $n<0$?

▸ **45.** [*M28*] The result of exercise 37 is somewhat surprising, since it implies that

$$\sum_{0\le k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor=\sum_{0\le k<m}\left\lfloor\frac{nk+x}{m}\right\rfloor.$$

This "reciprocity relationship" is one of many similar formulas (see Section 3.3.3). Show that for any function f, we have

$$\sum_{0\le j<n}f\left(\left\lfloor\frac{mj}{n}\right\rfloor\right)=\sum_{0\le r<m}\left\lceil\frac{rn}{m}\right\rceil\bigl(f(r-1)-f(r)\bigr)+nf(m-1).$$

In particular, prove that

$$\sum_{0\le j<n}\binom{\lfloor mj/n\rfloor+1}{k}+\sum_{0\le j<m}\left\lceil\frac{jn}{m}\right\rceil\binom{j}{k-1}=n\binom{m}{k}.$$

[*Hint:* Consider the change of variable $r=\lfloor mj/n\rfloor$. Binomial coefficients $\binom{m}{k}$ are discussed in Section 1.2.6.]

46. [*M29*] (*General reciprocity law.*) Extend the formula of exercise 45 to obtain an expression for $\sum_{0\le j<\alpha n}f(\lfloor mj/n\rfloor)$, where α is *any* positive real number.

▸ **47.** [*M31*] When p is an odd prime number, the *Legendre symbol* $\left(\frac{q}{p}\right)$ is defined to be $+1$, 0, or -1, depending on whether $q^{(p-1)/2}\bmod p$ is 1, 0, or $p-1$. (Exercise 26 proves that these are the only possible values.)

a) Given that q is not a multiple of p, show that the numbers

$$(-1)^{\lfloor 2kq/p\rfloor}(2kq\bmod p),\qquad 0<k<p/2,$$

are congruent in some order to the numbers 2, 4, $\ldots$, $p-1$ (modulo p). Hence $\left(\frac{q}{p}\right)=(-1)^\sigma$ where $\sigma=\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor$.

b) Use the result of (a) to calculate $\left(\frac{2}{p}\right)$.

c) Given that q is odd, show that $\sum_{0\le k<p/2}\lfloor 2kq/p\rfloor\equiv\sum_{0\le k<p/2}\lfloor kq/p\rfloor$ (modulo 2). [*Hint:* Consider the quantity $\lfloor(p-1-2k)q/p\rfloor$.]

d) Use the general reciprocity formula of exercise 46 to obtain the *law of quadratic reciprocity*, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{(p-1)(q-1)/4}$, given that p and q are distinct odd primes.

48. [*M26*] Prove or disprove the following identities, for integers m and n:

$$\text{(a)}\ \left\lfloor\frac{m+n-1}{n}\right\rfloor=\left\lceil\frac{m}{n}\right\rceil;\qquad\text{(b)}\ \left\lfloor\frac{n+2-\lfloor n/25\rfloor}{3}\right\rfloor=\left\lfloor\frac{8n+24}{25}\right\rfloor.$$

49. [*M30*] Suppose the integer-valued function $f(x)$ satisfies the two simple laws (i) $f(x+1)=f(x)+1$; (ii) $f(x)=f(f(nx)/n)$ for all positive integers n. Prove that either $f(x)=\lfloor x\rfloor$ for all rational x, or $f(x)=\lceil x\rceil$ for all rational x.

1.2.5. Permutations and Factorials

A *permutation of n objects* is an arrangement of n distinct objects in a row. There are six permutations of three objects $\{a,b,c\}$:

$$a\,b\,c,\qquad a\,c\,b,\qquad b\,a\,c,\qquad b\,c\,a,\qquad c\,a\,b,\qquad c\,b\,a.\tag{1}$$

The properties of permutations are of great importance in the analysis of algorithms, and we will deduce many interesting facts about them later in this book.* Our first task is simply to *count* them: How many permutations of n objects are possible? There are n ways to choose the leftmost object, and once this choice has been made there are $n-1$ ways to select a different object to place next to it; this gives us $n(n-1)$ choices for the first two positions. Similarly, we find that there are $n-2$ choices for the third object distinct from the first two, and a total of $n(n-1)(n-2)$ possible ways to choose the first three objects. In general, if p_{nk} denotes the number of ways to choose k objects out of n and to arrange them in a row, we see that

$$p_{nk}=n(n-1)\ldots(n-k+1).\tag{2}$$

The total number of permutations is therefore $p_{nn}=n(n-1)\ldots(1)$.

The process of *constructing* all permutations of n objects in an inductive manner, assuming that all permutations of $n-1$ objects have been constructed,

* In fact, permutations are so important, Vaughan Pratt has suggested calling them "perms." As soon as Pratt's convention is established, textbooks of computer science will be somewhat shorter (and perhaps less expensive).

is very important in our applications. Let us rewrite (1) using the numbers $\{1,2,3\}$ instead of the letters $\{a,b,c\}$; the permutations are then

$$1\,2\,3,\quad 1\,3\,2,\quad 2\,1\,3,\quad 2\,3\,1,\quad 3\,1\,2,\quad 3\,2\,1. \tag{3}$$

Consider how to get from this array to the permutations of $\{1,2,3,4\}$. There are two principal ways to go from $n-1$ objects to n objects.

Method 1. For each permutation $a_1\,a_2\,\ldots\,a_{n-1}$ of $\{1,2,\ldots,n{-}1\}$, form n others by inserting the number n in all possible places, obtaining

$$n\,a_1\,a_2\,\ldots\,a_{n-1},\quad a_1\,n\,a_2\,\ldots\,a_{n-1},\quad \ldots,\quad a_1\,a_2\,\ldots\,n\,a_{n-1},\quad a_1\,a_2\,\ldots\,a_{n-1}\,n.$$

For example, from the permutation 2 3 1 in (3), we get 4 2 3 1, 2 4 3 1, 2 3 4 1, 2 3 1 4. It is clear that all permutations of n objects are obtained in this manner and that no permutation is obtained more than once.

Method 2. For each permutation $a_1\,a_2\,\ldots\,a_{n-1}$ of $\{1,2,\ldots,n{-}1\}$, form n others as follows: First construct the array

$$a_1\,a_2\,\ldots\,a_{n-1}\,\tfrac12,\quad a_1\,a_2\,\ldots\,a_{n-1}\,\tfrac32,\quad \ldots,\quad a_1\,a_2\,\ldots\,a_{n-1}\,(n-\tfrac12).$$

Then rename the elements of each permutation using the numbers $\{1,2,\ldots,n\}$, *preserving order*. For example, from the permutation 2 3 1 in (3) we get

$$2\,3\,1\,\tfrac12,\quad 2\,3\,1\,\tfrac32,\quad 2\,3\,1\,\tfrac52,\quad 2\,3\,1\,\tfrac72$$

and, renaming, we get

$$3\,4\,2\,1,\quad 3\,4\,1\,2,\quad 2\,4\,1\,3,\quad 2\,3\,1\,4.$$

Another way to describe this process is to take the permutation $a_1a_2\ldots a_{n-1}$ and a number k, $1\le k\le n$; add one to each a_j whose value is $\ge k$, thus obtaining a permutation $b_1b_2\ldots b_{n-1}$ of the elements $\{1,\ldots,k-1,k+1,\ldots,n\}$; then $b_1b_2\ldots b_{n-1}k$ is a permutation of $\{1,\ldots,n\}$.

Again it is clear that we obtain each permutation of n elements exactly once by this construction. Putting k at the left instead of the right, or putting k in any other fixed position, would obviously work just as well.

If p_n is the number of permutations of n objects, both of these methods show that $p_n = np_{n-1}$; this offers us two further proofs that $p_n = n(n-1)\ldots(1)$, as we already established in Eq. (2).

The important quantity p_n is called n *factorial* and it is written

$$n! = 1\cdot 2\cdot\ldots\cdot n = \prod_{k=1}^{n} k. \tag{4}$$

Our convention for vacuous products (Section 1.2.3) gives us the value

$$0! = 1, \tag{5}$$

and with this convention the basic identity

$$n! = (n-1)!\,n \tag{6}$$

is valid for all positive integers n.

Factorials come up sufficiently often in computer work that the reader is advised to memorize the values of the first few:

$$0! = 1,\quad 1! = 1,\quad 2! = 2,\quad 3! = 6,\quad 4! = 24,\quad 5! = 120.$$

The factorials increase very rapidly; for example, 1000! is an integer with over 2500 decimal digits.

It is helpful to keep the value $10! = 3{,}628{,}800$ in mind; one should remember that 10! is about $3\frac12$ million. In a sense, this number represents an approximate dividing line between things that are practical to compute and things that are not. If an algorithm requires the testing of more than 10! cases, it may consume too much computer time to be practical. On the other hand, if we decide to test 10! cases and each case requires, say, one millisecond of computer time, then the entire run will take about an hour. These comments are very vague, of course, but they can be useful to give an intuitive idea of what is computationally feasible.

It is only natural to wonder what relation $n!$ bears to other quantities in mathematics. Is there any way to tell how large 1000! is, without laboriously carrying out the multiplications implied in Eq. (4)? The answer was found by James Stirling in his famous work *Methodus Differentialis* (1730), page 137; we have

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n}. \tag{7}$$

The "$\approx$" sign that appears here denotes "approximately equal," and "e" is the base of natural logarithms introduced in Section 1.2.2. We will prove Stirling's approximation (7) in Section 1.2.11.2. Exercise 24 gives a simple proof of a less precise result.

As an example of the use of this formula, we may compute

$$40320 = 8! \approx 4\sqrt{\pi}\left(\frac{8}{e}\right)^{8} = 2^{26}\sqrt{\pi}\,e^{-8} \approx 67108864\cdot 1.77245\cdot 0.00033546 \approx 39902.$$

In this case the error is about 1%; we will see later that the relative error is approximately $1/(12n)$.

In addition to the approximate value given by Eq. (7), we can also rather easily obtain the exact value of $n!$ factored into primes. In fact, the prime p is a divisor of $n!$ with the multiplicity

$$\mu = \left\lfloor\frac{n}{p}\right\rfloor + \left\lfloor\frac{n}{p^2}\right\rfloor + \left\lfloor\frac{n}{p^3}\right\rfloor + \cdots = \sum_{k>0}\left\lfloor\frac{n}{p^k}\right\rfloor. \tag{8}$$

For example, if $n = 1000$ and $p = 3$, we have

$$\begin{aligned}\mu &= \left\lfloor\frac{1000}{3}\right\rfloor + \left\lfloor\frac{1000}{9}\right\rfloor + \left\lfloor\frac{1000}{27}\right\rfloor + \left\lfloor\frac{1000}{81}\right\rfloor + \left\lfloor\frac{1000}{243}\right\rfloor + \left\lfloor\frac{1000}{729}\right\rfloor\\ &= 333 + 111 + 37 + 12 + 4 + 1 = 498,\end{aligned}$$

so 1000! is divisible by 3^{498} but not by 3^{499}. Although formula (8) is written as an infinite sum, it is really finite for any particular values of n and p, because all of the terms are eventually zero. It follows from exercise 1.2.4–35 that $\lfloor n/p^{k+1}\rfloor = \lfloor \lfloor n/p^k\rfloor /p\rfloor$; this fact facilitates the calculation in Eq. (8), since we can just divide the value of the previous term by p and discard the remainder.

Equation (8) follows from the fact that $\lfloor n/p^k\rfloor$ is the number of integers among $\{1,2,\ldots,n\}$ that are multiples of p^k. If we study the integers in the product (4), any integer that is divisible by p^j but not by p^{j+1} is counted exactly j times: once in $\lfloor n/p\rfloor$, once in $\lfloor n/p^2\rfloor$, $\ldots$, once in $\lfloor n/p^j\rfloor$. This accounts for all occurrences of p as a factor of $n!$.

Another natural question arises: Now that we have defined $n!$ for nonnegative integers n, perhaps the factorial function is meaningful also for rational values of n, and even for real values. What is $(\frac{1}{2})!$, for example? Let us illustrate this point by introducing the "termial" function

$$n? = 1 + 2 + \cdots + n = \sum_{k=1}^{n} k, \tag{9}$$

which is analogous to the factorial function except that we are adding instead of multiplying. We already know the sum of this arithmetic progression from Eq. 1.2.3–(15):

$$n? = \tfrac{1}{2}n(n+1). \tag{10}$$

This suggests a good way to generalize the "termial" function to arbitrary n, by using (10) instead of (9). We have $(\frac{1}{2})? = \frac{3}{8}$.

Stirling himself made several attempts to generalize $n!$ to noninteger n. He extended the approximation (7) into an infinite sum, but unfortunately the sum did not converge for any value of n; his method gave extremely good approximations, but it couldn't be extended to give an *exact* value. [For a discussion of this somewhat unusual situation, see K. Knopp, *Theory and Application of Infinite Series*, 2nd ed. (Glasgow: Blackie, 1951), 518–520, 527, 534.]

Stirling tried again, by noticing that

$$\begin{aligned} n! = 1 &+ \Bigl(1 - \frac{1}{1!}\Bigr)n + \Bigl(1 - \frac{1}{1!} + \frac{1}{2!}\Bigr)n(n-1) \\ &+ \Bigl(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!}\Bigr)n(n-1)(n-2) + \cdots. \end{aligned} \tag{11}$$

(We will prove this formula in the next section.) The apparently infinite sum in Eq. (11) is in reality finite for any nonnegative integer n; however, it does not provide the desired generalization of $n!$, since the infinite sum does not exist *except* when n is a nonnegative integer. (See exercise 16.)

Still undaunted, Stirling found a sequence $a_1, a_2, \ldots$ such that

$$\ln n! = a_1 n + a_2 n(n-1) + \cdots = \sum_{k\ge 0} a_{k+1} \prod_{0\le j\le k} (n-j). \tag{12}$$

He was unable to *prove* that this sum defined $n!$ for all fractional values of n, although he was able to deduce the value of $(\frac{1}{2})! = \sqrt{\pi}/2$.

At about the same time, Leonhard Euler considered the same problem, and he was the first to find the appropriate generalization:

$$n! = \lim_{m\to\infty} \frac{m^n m!}{(n+1)(n+2)\ldots(n+m)}. \tag{13}$$

Euler communicated this idea in a letter to Christian Goldbach on October 13, 1729. His formula defines $n!$ for any value of n except negative integers (when the denominator becomes zero); in such cases $n!$ is taken to be infinite. Exercises 8 and 22 explain why Eq. (13) is a reasonable definition.

Nearly two centuries later, in 1900, C. Hermite proved that Stirling's idea (12) actually does define $n!$ successfully for nonintegers n, and that in fact Euler's and Stirling's generalizations are identical.

Many notations were used for factorials in the early days. Euler actually wrote $[n]$, Gauss wrote $\Pi\, n$, and the symbols $\underline{\lfloor n}$ and $\underline{n\rfloor}$ were popular in England and Italy. The notation $n!$, which is universally used today when n is an integer, was introduced by a comparatively little known mathematician, Christian Kramp, in an algebra text [*Élémens d'Arithmétique Universelle* (Cologne: 1808)].

When n is *not* an integer, however, the notation $n!$ is less common; instead we customarily employ a notation due to A. M. Legendre:

$$n! = \Gamma(n+1) = n\Gamma(n). \tag{14}$$

This function $\Gamma(x)$ is called the *gamma function*, and by Eq. (13) we have the definition

$$\Gamma(x) = \frac{x!}{x} = \lim_{m\to\infty} \frac{m^x m!}{x(x+1)(x+2)\ldots(x+m)}. \tag{15}$$

A graph of $\Gamma(x)$ is shown in Fig. 7.

Equations (13) and (15) define factorials and the gamma function for complex values as well as real values; but we generally use the letter z, instead of n or x, when thinking of a variable that has both real and imaginary parts. The factorial and gamma functions are related not only by the rule $z! = \Gamma(z+1)$ but also by

$$(-z)!\,\Gamma(z) = \frac{\pi}{\sin \pi z}, \tag{16}$$

which holds whenever z is not an integer. (See exercise 23.)

Although $\Gamma(z)$ is infinite when z is zero or a negative integer, the function $1/\Gamma(z)$ is well defined for all complex z. (See exercise 1.2.7–24.) Advanced applications of the gamma function often make use of an important contour integral formula due to Hermann Hankel:

$$\frac{1}{\Gamma(z)} = \frac{1}{2\pi i}\oint \frac{e^t\,dt}{t^z}; \tag{17}$$

the path of complex integration starts at $-\infty$, then circles the origin in a counterclockwise direction and returns to $-\infty$. [*Zeitschrift für Math. und Physik* **9** (1864), 1–21.]

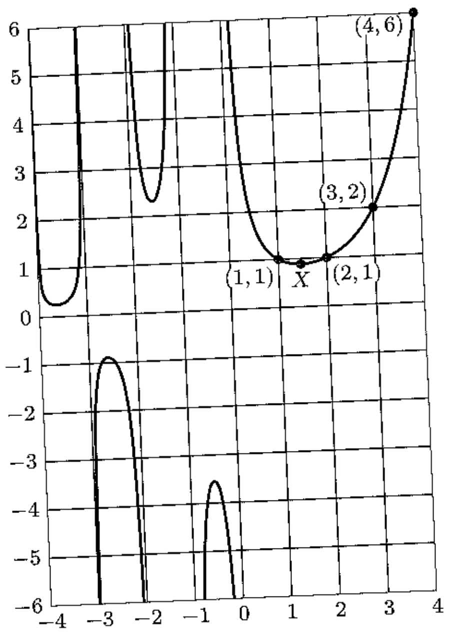

Fig. 7. The function $\Gamma(x) = (x-1)!$. The local minimum at X has the coordinates $(1.46163\,21449\,68362\,34126\,26595,\ 0.88560\,31944\,10888\,70027\,88159)$.

Many formulas of discrete mathematics involve factorial-like products known as *factorial powers*. The quantities $x^{\underline{k}}$ and $x^{\overline{k}}$ (read, "x to the k falling" and "x to the k rising") are defined as follows, when k is a positive integer:

$$x^{\underline{k}} = x(x-1)\ldots(x-k+1) = \prod_{j=0}^{k-1}(x-j); \tag{18}$$

$$x^{\overline{k}} = x(x+1)\ldots(x+k-1) = \prod_{j=0}^{k-1}(x+j); \tag{19}$$

Thus, for example, the number p_{nk} of (2) is just $n^{\underline{k}}$. Notice that we have

$$x^{\overline{k}} \;=\; (x+k-1)^{\underline{k}} \;=\; (-1)^k(-x)^{\underline{k}}. \tag{20}$$

The general formulas

$$x^{\underline{k}} = \frac{x!}{(x-k)!}, \qquad x^{\overline{k}} = \frac{\Gamma(x+k)}{\Gamma(x)} \tag{21}$$

can be used to define factorial powers for other values of k. [The notations $x^{\overline{k}}$ and $x^{\underline{k}}$ are due respectively to A. Capelli, *Giornale di Mat. di Battaglini* **31** (1893), 291–313, and L. Toscano, *Comment. Accademia della Scienze* **3** (1939), 721–757.]

The interesting history of factorials from the time of Stirling to the present day is traced in an article by P. J. Davis, "Leonhard Euler's integral: A historical profile of the gamma function," *AMM* **66** (1959), 849–869. See also J. Dutka, *Archive for History of Exact Sciences* **31** (1984), 15–34.

EXERCISES

1. [*00*] How many ways are there to shuffle a 52-card deck?

2. [*10*] In the notation of Eq. (2), show that $p_{n(n-1)} = p_{nn}$, and explain why this happens.

3. [*10*] What permutations of $\{1,2,3,4,5\}$ would be constructed from the permutation 3 1 2 4 using Methods 1 and 2, respectively?

▸ **4.** [*13*] Given the fact that $\log_{10} 1000! = 2567.60464\ldots$, determine exactly how many decimal digits are present in the number 1000!. What is the *most significant* digit? What is the *least significant* digit?

5. [*15*] Estimate 8! using the following more exact version of Stirling's approximation:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\left(1+\frac{1}{12n}\right).$$

▸ **6.** [*17*] Using Eq. (8), write 20! as a product of prime factors.

7. [*M10*] Show that the "generalized termial" function in Eq. (10) satisfies the identity $x? = x + (x-1)?$ for all real numbers x.

8. [*HM15*] Show that the limit in Eq. (13) does equal $n!$ when n is a nonnegative integer.

9. [*M10*] Determine the values of $\Gamma(\frac{1}{2})$ and $\Gamma(-\frac{1}{2})$, given that $(\frac{1}{2})! = \sqrt{\pi}/2$.

▸ **10.** [*HM20*] Does the identity $\Gamma(x+1) = x\Gamma(x)$ hold for all real numbers x? (See exercise 7.)

11. [*M15*] Let the representation of n in the binary system be $n = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r}$, where $e_1 > e_2 > \cdots > e_r \geq 0$. Show that $n!$ is divisible by 2^{n-r} but not by 2^{n-r+1}.

▸ **12.** [*M22*] (A. Legendre, 1808.) Generalizing the result of the previous exercise, let p be a prime number, and let the representation of n in the p-ary number system be $n = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0$. Express the number μ of Eq. (8) in a simple formula involving n, p, and a's.

13. [*M23*] (*Wilson's theorem*, actually due to Leibniz, 1682.) If p is prime, then $(p-1)! \bmod p = p-1$. Prove this, by pairing off numbers among $\{1,2,\ldots,p-1\}$ whose product modulo p is 1.

▸ **14.** [*M28*] (L. Stickelberger, 1890.) In the notation of exercise 12, we can determine $n! \bmod p$ in terms of the p-ary representation, for *any* positive integer n, thus generalizing Wilson's theorem. In fact, prove that $n!/p^{\mu} \equiv (-1)^{\mu} a_0!\,a_1!\ldots a_k!$ (modulo p).

15. [*HM15*] The *permanent* of a square matrix is defined by the same expansion as the determinant except that each term of the permanent is given a plus sign while the determinant alternates between plus and minus. Thus the permanent of

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

is $aei + bfg + cdh + gec + hfa + idb$. What is the permanent of

$$\begin{pmatrix} 1\times 1 & 1\times 2 & \ldots & 1\times n \\ 2\times 1 & 2\times 2 & \ldots & 2\times n \\ \vdots & \vdots & \ddots & \vdots \\ n\times 1 & n\times 2 & \ldots & n\times n \end{pmatrix}?$$