Generating Permutations. Ranking and Unranking Permutations. The Pigeonhole Principle. The Inclusion and Exclusion Principle

Isabela Drămnesc UVT

Computer Science Department,
West University of Timișoara,
Romania

08 October 2018

Remember from Lecture 1 that ...

If A is a finite set with n elements then

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.
- A combination of r out of n from A is a subset with r elements from A.

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.
- A combination of r out of n from A is a subset with r elements from A.

Example ($A = \{a_1, a_2, a_3\}$)

- The 2-permutations of A are (order is important!):
- The 2-combinations of A are (order is irrelevant!):
- The permutations of A are:

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.
- A combination of r out of n from A is a subset with r elements from A.

Example ($A = \{a_1, a_2, a_3\}$)

- The 2-permutations of A are (order is important!): $\langle a_1, a_2\rangle, \langle a_2, a_1\rangle, \langle a_1, a_3\rangle, \langle a_3, a_1\rangle, \langle a_2, a_3\rangle, \langle a_3, a_1\rangle$
- The 2-combinations of A are (order is irrelevant!):
- The permutations of A are:

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.
- A combination of r out of n from A is a subset with r elements from A.

Example ($A = \{a_1, a_2, a_3\}$)

- The 2-permutations of A are (order is important!): $\langle a_1, a_2\rangle, \langle a_2, a_1\rangle, \langle a_1, a_3\rangle, \langle a_3, a_1\rangle, \langle a_2, a_3\rangle, \langle a_3, a_1\rangle$
- The 2-combinations of A are (order is irrelevant!): $\{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}$
- The permutations of A are:

Remember from Lecture 1 that ...

If A is a finite set with n elements then

- An arrangement of r out of n (or r-permutation) of A is an ordered sequence of elements from A.
  - A permutation of A is an ordered sequence of all elements of A.
- A combination of r out of n from A is a subset with r elements from A.

Example ($A = \{a_1, a_2, a_3\}$)

- The 2-permutations of A are (order is important!):
  $\langle a_1, a_2\rangle, \langle a_2, a_1\rangle, \langle a_1, a_3\rangle, \langle a_3, a_1\rangle, \langle a_2, a_3\rangle, \langle a_3, a_1\rangle$
- The 2-combinations of A are (order is irrelevant!):
  $\{a_1, a_2\}, \{a_1, a_3\}, \{a_2, a_3\}$
- The permutations of A are:
  $\langle a_1, a_2, a_3\rangle$, $\langle a_1, a_3, a_2\rangle$, $\langle a_2, a_1, a_3\rangle$, $\langle a_2, a_3, a_1\rangle$,
  $\langle a_3, a_1, a_2\rangle$, $\langle a_3, a_2, a_1\rangle$

Operations with permutations

In the first part of this lecture we will learn

- How to order permutations, such that we can talk about:
  - ▷ the first permutation, the second permutation, a.s.o.
- How to generate directly the k-th permutation
- How to find directly the rank of a given permutation.

Relations of order for r-permutations

Assume A is a finite set with n elements.

1. First, we order the elements of set A

   $\Rightarrow$ $A = \{a_1, a_2, \ldots, a_n\}$ where
   a_1 = first element
   ...
   a_n = the n-th element.

   $\Rightarrow$ A becomes an ordered set (an alphabet) in which $a_1 < a_2 < \ldots < a_n$.

2. the r-permutations are "words" $\langle b_1, ..., b_r\rangle$ of length r which we order like the words in a dictionary, for example:

   $$\langle a_1, a_2\rangle < \langle a_1, a_3\rangle < \langle a_2, a_1\rangle < \ldots$$

   This way of ordering r-permutations is called lexicographic ordering:

   $\langle b_1, \ldots, b_r\rangle < \langle c_1, \ldots, c_r\rangle$ if there is a position k such that $b_i = c_i$ for $1 \leq i < k$, and $b_k < c_k$.

Let $A = \{a_1, \dots, a_n\}$ be an ordered set with $a_1 < \dots < a_n$ and $N = \{1, 2, \dots, n\}$.

1. The r-permutations of A are "words" of the form $\langle a_{i_1}, \dots, a_{i_r} \rangle$ with $i_1, \dots, i_r \in N$.
2. $\langle a_{i_1}, \dots, a_{i_r} \rangle$ is an r-permutation of A if and only if $(i_1, \dots, i_r)$ is an r-permutation of N.
3. $\langle a_{i_1}, \dots, a_{i_r} \rangle < \langle a_{j_1}, \dots, a_{j_r} \rangle$ if and only if $\langle i_1, \dots, i_r \rangle < \langle j_1, \dots, j_r \rangle$.

$\Rightarrow$ it is sufficient to know how to order and to enumerate the r-permutations of numbers from the set N.

From now on we will consider only the r-permutations of the ordered set $A = \{1, \dots, n\}$.

Rank of an r-permutation

The rank of an r-permutation is the position where the r-permutation occurs in lexicographic order, starting from position 0.

Example ($A = \{1, 2, 3\}$)

2-permutation	rank	permutation	rank
$\langle 1, 2\rangle$	0	$\langle 1, 2, 3\rangle$	0
$\langle 1, 3\rangle$	1	$\langle 1, 3, 2\rangle$	1
$\langle 2, 1\rangle$	2	$\langle 2, 1, 3\rangle$	2
$\langle 2, 3\rangle$	3	$\langle 2, 3, 1\rangle$	3
$\langle 3, 1\rangle$	4	$\langle 3, 1, 2\rangle$	4
$\langle 3, 2\rangle$	5	$\langle 3, 2, 1\rangle$	5

Generating the next permutation in lexicographic order

Problem

How can we compute directly (and reasonably fast) the permutation of $N = \{1, \ldots, n\}$ that is after the permutation $\langle p_1, \ldots, p_n \rangle$ in lexicographic order?

Example ($N = \{1, 2, 3, 4, 5\}$)

permutation	next permutation
$\langle 5, 1, 3, 2, 4 \rangle$	
$\langle 5, 2, 4, 3, 1 \rangle$	
$\langle 5, 4, 3, 2, 1 \rangle$	

Generating the next permutation in lexicographic order

Problem

How can we compute directly (and reasonably fast) the permutation of $N = \{1, \ldots, n\}$ that is after the permutation $\langle p_1, \ldots, p_n \rangle$ in lexicographic order?

Example ($N = \{1, 2, 3, 4, 5\}$)

permutation	next permutation
$\langle 5, 1, 3, 2, 4 \rangle$	$\langle 5, 1, 3, 4, 2 \rangle$
$\langle 5, 2, 4, 3, 1 \rangle$	
$\langle 5, 4, 3, 2, 1 \rangle$	

Problem

How can we compute directly (and reasonably fast) the permutation of $N = \{1, \ldots, n\}$ that is after the permutation $\langle p_1, \ldots, p_n \rangle$ in lexicographic order?

Example ($N = \{1, 2, 3, 4, 5\}$)

permutation	next permutation
$\langle 5, 1, 3, 2, 4 \rangle$	$\langle 5, 1, 3, 4, 2 \rangle$
$\langle 5, 2, 4, 3, 1 \rangle$	$\langle 5, 3, 1, 2, 4 \rangle$
$\langle 5, 4, 3, 2, 1 \rangle$	

Generating the next permutation in lexicographic order

Problem

How can we compute directly (and reasonably fast) the permutation of $N = \{1, \ldots, n\}$ that is after the permutation $\langle p_1, \ldots, p_n \rangle$ in lexicographic order?

Example ($N = \{1, 2, 3, 4, 5\}$)

permutation	next permutation
$\langle 5, 1, 3, 2, 4 \rangle$	$\langle 5, 1, 3, 4, 2 \rangle$
$\langle 5, 2, 4, 3, 1 \rangle$	$\langle 5, 3, 1, 2, 4 \rangle$
$\langle 5, 4, 3, 2, 1 \rangle$	none

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.
3. Permute p_j with p_{i-1}, and then reverse the suffix $p_i, \ldots, p_n$.

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.
3. Permute p_j with p_{i-1}, and then reverse the suffix $p_i, \ldots, p_n$.

Example

$$\langle p_1, p_2, p_3, p_4, p_5 \rangle = \langle 5, 2, 4, 3, 1 \rangle$$

$$\langle 5, 2, \underset{\uparrow\, i=3}{\color{red}{4}}, \color{red}{3}, \color{red}{1} \rangle$$

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.
3. Permute p_j with p_{i-1}, and then reverse the suffix $p_i, \ldots, p_n$.

Example

$\langle p_1, p_2, p_3, p_4, p_5 \rangle = \langle 5, 2, 4, 3, 1 \rangle$

$\langle 5, 2, 4, 3, 1 \rangle$

swap values of $p_{i-1} = 2$ and $p_j = 3$

$i = 3 \quad j = 4$

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.
3. Permute p_j with p_{i-1}, and then reverse the suffix $p_i, \ldots, p_n$.

Example

$\langle p_1, p_2, p_3, p_4, p_5 \rangle = \langle 5, 2, 4, 3, 1 \rangle$

$\langle 5, 3, 4, 2, 1 \rangle$ invert $\langle p_i, \ldots, p_n \rangle = \langle 4, 2, 1 \rangle$

$i = 3$

The permutation after $\langle p_1, \ldots, p_n \rangle$ in lexicographic order can be computed as follows:

1. Find i such that $p_i > \ldots > p_n$ is the longest decreasing suffix of $\langle p_1, \ldots, p_n \rangle$
2. Find $j \geq i$ such that p_j is the smallest number greater than p_{i-1}.
3. Permute p_j with p_{i-1}, and then reverse the suffix $p_i, \ldots, p_n$.

Example

$$\langle p_1, p_2, p_3, p_4, p_5 \rangle = \langle 5, 2, 4, 3, 1 \rangle$$

$$\langle 5, 3, 1, 2, 4 \rangle \quad = \text{next permutation}$$

NextPermutation(p: int[0 .. $n-1$])
$i := n-2$;
while $(p[i] > p[i+1])$
    i--;
$j := n-1$;
while $(p[j] < p[i])$
    j--;
// swap $p[i]$ with $p[j]$
$tmp := p[i]$;
$p[i] := p[j]$;
$p[j] := tmp$;
// revert (p[i+1], ..., p[n-1])
for $(k := 0;\ k < \lfloor (n-i-1)/2 \rfloor;\ k{+}{+})$
        // swap $p[i+1+k]$ with $p[n-1-k]$
        $tmp := p[i+1+k]$;
        $p[i+1+k] := p[n-1-k]$;
        $p[n-1-k] := tmp$;
return p;

Operations with permutations

Problems

1. How to compute directly the rank of a permutation $\langle p_1, \dots, p_n \rangle$ of $N = \{1, \dots, n\}$ in lexicographic order?
2. How to compute directly the permutation $\langle p_1, \dots, p_n \rangle$ of $N = \{1, \dots, n\}$ with rank k?
   Note that the rank is a number between 0 and $n! - 1$.

Computing the rank of a permutation

- Let r be the rank of a permutation $\langle p_1, \ldots, p_n \rangle$.
  - ▷ If $p_1 = 1$ then $0 \leq r < (n-1)!$
  - ▷ If $p_1 = 2$ then $(n-1)! \leq r < 2 \cdot (n-1)!$

    ...
  - ▷ If $p_1 = k$ then $(k-1) \cdot (n-1)! \leq r < k \cdot (n-1)!$

    ...
  - ▷ If $p_1 = n$ then $(n-1) \cdot (n-1)! \leq r < n \cdot (n-1)! = n!$

Computing the rank of a permutation

- Let r be the rank of a permutation $\langle p_1, \ldots, p_n \rangle$.
  - ▷ If $p_1 = 1$ then $0 \leq r < (n-1)!$
  - ▷ If $p_1 = 2$ then $(n-1)! \leq r < 2 \cdot (n-1)!$

    ...
  - ▷ If $p_1 = k$ then $(k-1) \cdot (n-1)! \leq r < k \cdot (n-1)!$

    ...
  - ▷ If $p_1 = n$ then $(n-1) \cdot (n-1)! \leq r < n \cdot (n-1)! = n!$

$\Rightarrow$ in general, $(p_1 - 1) \cdot (n-1)! \leq r < p_1 \cdot (n-1)!$

Computing the rank of a permutation

- Let r be the rank of a permutation $\langle p_1, \ldots, p_n \rangle$.
  - ▷ If $p_1 = 1$ then $0 \leq r < (n-1)!$
  - ▷ If $p_1 = 2$ then $(n-1)! \leq r < 2 \cdot (n-1)!$

    ...
  - ▷ If $p_1 = k$ then $(k-1) \cdot (n-1)! \leq r < k \cdot (n-1)!$

    ...
  - ▷ If $p_1 = n$ then $(n-1) \cdot (n-1)! \leq r < n \cdot (n-1)! = n!$

$\Rightarrow$ in general, $(p_1 - 1) \cdot (n-1)! \leq r < p_1 \cdot (n-1)!$

$\Rightarrow$ rank of $\langle p_1, \ldots, p_n \rangle =$ $(p_1 - 1) \cdot (n-1)! +$ rank of $\langle p_2, \ldots, p_n \rangle$ in the lexicographic enumeration of the permutations of $N - \{p_1\}$

- Let r be the rank of a permutation $\langle p_1, \ldots, p_n \rangle$.
  - ▷ If $p_1 = 1$ then $0 \leq r < (n-1)!$
  - ▷ If $p_1 = 2$ then $(n-1)! \leq r < 2 \cdot (n-1)!$

    ...
  - ▷ If $p_1 = k$ then $(k-1) \cdot (n-1)! \leq r < k \cdot (n-1)!$

    ...
  - ▷ If $p_1 = n$ then $(n-1) \cdot (n-1)! \leq r < n \cdot (n-1)! = n!$

$\Rightarrow$ in general, $(p_1 - 1) \cdot (n-1)! \leq r < p_1 \cdot (n-1)!$

$\Rightarrow$ rank of $\langle p_1, \ldots, p_n \rangle =$ $(p_1 - 1) \cdot (n-1)! +$ rank of $\langle p_2, \ldots, p_n \rangle$ in the lexicographic enumeration of the permutations of $N - \{p_1\}$

$\Rightarrow$ r can be computed recursively.

Computing the rank of a permutation

Example

- The permutation $\langle p_1, p_2, p_3, p_4, p_5 \rangle = \langle 2, 3, 1, 5, 4 \rangle$ has rank

  $r = (2-1) \cdot (5-1)! +$ rank of $\langle 3, 1, 5, 4 \rangle$ in the lex. order of the permutations of $\{1, 3, 4, 5\}$.

  - rank of $\langle 3, 1, 5, 4 \rangle$ in the lex. order of the permutations of $\{1, 3, 4, 5\}$ coincides with
    rank of $\langle 2, 1, 4, 3 \rangle$ in the lex. order of the permutations of $\{1, 2, 3, 4\}$

    (the values of all elements $p_1 = 2$ were decreased by 1)

- By recursion, we find out that the rank of $\langle 2, 1, 4, 3 \rangle$ is 7.

  $\Rightarrow$ rank of $\langle 2, 3, 1, 5, 4 \rangle$ is $24 + 7 = 31$.

```
Rank(p : int[0 .. n-1])
if n == 1
    return 0
else
   q : int[0 .. n-2];
   // adjust p[1..n-1] to become a permutation of {1,...,n-1}
   // memorized in the array q[0 .. n-2]
   for(i := 1; i ≤ n-1; i++)
       if(p[i] < p[0])
           q[i-1] = p[i];
       else
           q[i-1] = p[i]-1;
   return Rank[q] + (p[0]-1)·(n-1)!
```

Computing the permutation with a given rank

We look for an algorithm to compute directly the permutation $\langle p_1, \ldots, p_n \rangle$ with rank r when $0 \leq r < n!$.

- We already noticed that if the permutation $\langle p_1, \ldots, p_n \rangle$ has rank r, then $(p_1 - 1) \cdot (n-1)! \leq r < p_1 \cdot (n-1)!$

$\Rightarrow$ $p_1 = \left\lfloor \dfrac{r}{(n-1)!} \right\rfloor + 1$

$\Rightarrow$ If $(q_1, \ldots, q_{n-1})$ is the permutation with rank $r - (p_1 - 1) \cdot (n-1)!$ then

$$p_{i+1} = \begin{cases} q_i & \text{if } q_i < p_1, \\ q_i + 1 & \text{if } q_i \geq p_1. \end{cases}$$

for all $1 \leq i < n$.

Minimum change permutations

- There are many other orders to generate all permutations, different from the lexicographic order.
- Often, we want the fast generation of all permutations:
  - ▷ This means to generate very fast the next permutation from the previous one.
  - ▷ In 1963, Heap discovered an algorithm that generates the next permutation by exchanging the values of only two elements.

Heap's algorithm is the fastest known algorithm to generate all permutations.

for($i := 1; i \leq n; i{+}{+}$)
    $p[i] := i$
for($c := 1; c \leq n; c{+}{+}$)
    1. generate all permutations $\langle p[1], \ldots, p[n-1]\rangle$ without modifying $p[n]$;
      (at the end of step 1, p contains the last generated permutation)
    2. swap the value of $p[n]$ with that of $p[f(n,c)]$

$$\text{where } f(n,c) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ c & \text{if } n \text{ is even.} \end{cases}$$

for($i := 1; i \leq n; i$++)
  $p[i] := i$
for($c := 1; c \leq n; c$++)
  1. generate all permutations $\langle p[1], \ldots, p[n-1]\rangle$ without modifying $p[n]$;
   (at the end of step 1, p contains the last generated permutation)
  2. swap the value of $p[n]$ with that of $p[f(n,c)]$

$$\text{where } f(n,c) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ c & \text{if } n \text{ is even.} \end{cases}$$

REMARKS

for($i := 1; i \leq n; i$++)
  $p[i] := i$
for($c := 1; c \leq n; c$++)
  1. generate all permutations $\langle p[1], \ldots, p[n-1] \rangle$ without modifying $p[n]$;
   (at the end of step 1, p contains the last generated permutation)
  2. swap the value of $p[n]$ with that of $p[f(n,c)]$

$$\text{where } f(n,c) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ c & \text{if } n \text{ is even.} \end{cases}$$

Remarks

- Heap's algorithm generates all permutations of $\{1, \ldots, n\}$ in an order different from the lexicographic order.

for$(i := 1; i \leq n; i{+}{+})$
  $p[i] := i$
for$(c := 1; c \leq n; c{+}{+})$
  1. generate all permutations $\langle p[1], \ldots, p[n-1] \rangle$ without modifying $p[n]$;
    (at the end of step 1, p contains the last generated permutation)
  2. swap the value of $p[n]$ with that of $p[f(n,c)]$

$$\text{where } f(n,c) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ c & \text{if } n \text{ is even.} \end{cases}$$

REMARKS

- Heap's algorithm generates all permutations of $\{1, \ldots, n\}$ in an order different from the lexicographic order.
- Every permutation differs from the previous one by a transposition (that is, a swap of the values of 2 elements).

for($i := 1; i \leq n; i$++)
    $p[i] := i$
for($c := 1; c \leq n; c$++)
    1. generate all permutations $\langle p[1], \ldots, p[n-1] \rangle$ without modifying $p[n]$;
      (at the end of step 1, p contains the last generated permutation)
    2. swap the value of $p[n]$ with that of $p[f(n,c)]$

$$\text{where } f(n,c) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ c & \text{if } n \text{ is even.} \end{cases}$$

REMARKS

- Heap's algorithm generates all permutations of $\{1, \ldots, n\}$ in an order different from the lexicographic order.
- Every permutation differs from the previous one by a transposition (that is, a swap of the values of 2 elements).

Example

Heap's algorithm enumerates the permutations of $\{1,2,3\}$ in the following order:

$$\langle 1,2,3 \rangle, \langle 2,1,3 \rangle, \langle 3,1,2 \rangle, \langle 1,3,2 \rangle, \langle 2,3,1 \rangle, \langle 3,2,1 \rangle$$

Exercises (part 1)

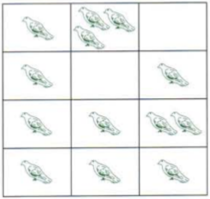
1. Write a program which reads a sequence of n numbers, and then it displays:
   - "a permutation" if the sequence is a permutation of $\{1, \ldots, n\}$
   - "not a permutation" otherwise.
2. Write a program which reads numbers n and $r \in \{0, 1, \ldots, n! - 1\}$, and then it displays the permutation $\{1, \ldots, n\}$ with rank r.
3. Write a program which reads a permutation of $\{1, \ldots, n\}$ and it displays the rank of that permutation.
4. Write a program which reads a permutation $\langle a_1, \ldots, a_n \rangle$ and computes its *inverse*, that is, the permutation $\langle b_1, \ldots, b_n \rangle$ such that $b_{a_i} = a_{b_i} = i$ for all $1 \leq i \leq n$.

Exercises (part 2)

1. Write a program which reads a permutation and computes the next permutation in lexicographic order.
2. Write a program which reads a permutation and computes the previous permutation in lexicographic order.

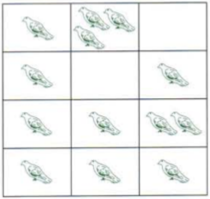
The Pigeonhole Principle

- Suppose that a flock of 13 pigeons flies into a set of 12 pigeonholes.
- The number of holes is smaller than the number of pigeons $\Rightarrow$ at least one pigeonhole must have at least 2 pigeons in it.



The Pigeonhole Principle

- Suppose that a flock of 13 pigeons flies into a set of 12 pigeonholes.
- The number of holes is smaller than the number of pigeons $\Rightarrow$ at least one pigeonhole must have at least 2 pigeons in it.



The Pigeonhole Principle (or Dirichlet's Principle)

Let n be a positive integer. If more than n objects are distributed among n containers, then some container must contain more than one object.

Establish the existence of a particular configuration or combination in many situations.

1. Suppose 367 freshmen are enrolled in the lecture on combinatorics. Then two of them must have the same birthday.

   PROOF. There are more freshmen than calendaristic days. By pigeonhole principle, at least 2 freshmen were born in same calendaristic day.

2. n boxers did compete in a round-robin tournament. We know that no contestant was undefeated. Then two boxers must have the same record in the tournament.

   PROOF. There are n boxers, and every boxer has between 0 and $n-2$ wins. (Note that no boxer has $n-1$ wins, because we know that no boxer was undefeated.)
   By pigeonhole principle, at least 2 boxers must have the same winning record.

Generalization: Let m and n be positive integers. If more than $m \cdot n$ objects are distributed among n containers, then at least one container must contain at least $m+1$ objects.

PROOF: by contradiction. If we place at most m objects in all containers, then the total number of objects would be at most $m \cdot n$.

Theorem

If $a_1, a_2, \ldots, a_n \in \mathbb{R}$ and $\mu = \dfrac{a_1 + a_2 + \ldots + a_n}{n}$, then there exist integers i and j with $1 \leq i, j \leq n$ such that $a_i \leq \mu$ and $a_j \geq \mu$.

PROOF: by contradiction.

- If every element is strictly greater than μ then $\mu = (a_1 + a_2 + \ldots + a_n)/n > \dfrac{n \cdot \mu}{n} = \mu$, contradiction $\Rightarrow \exists a_i \leq \mu$.
- If every element is strictly smaller than μ then $\mu = (a_1 + a_2 + \ldots + a_n)/n < \dfrac{n \cdot \mu}{n} = \mu$, contradiction $\Rightarrow \exists a_j \geq \mu$.

Definition (Monotonic sequence)

A sequence $a_1, a_2, \ldots, a_n$ is

- increasing if $a_1 \leq a_2 \leq \ldots \leq a_n$
- strictly increasing if $a_1 < a_2 < \ldots < a_n$
- decreasing if $a_1 \geq a_2 \geq \ldots \geq a_n$
- strictly decreasing if $a_1 > a_2 > \ldots > a_n$

- Consider the sequence $3, 5, 8, 10, 6, 1, 9, 2, 7, 4.$
- What are the increasing subsequences of maximal length?

$$\langle 3, 5, 8, 10 \rangle, \langle 3, 5, 8, 9 \rangle, \langle 3, 5, 6, 7 \rangle, \langle 3, 5, 6, 9 \rangle$$

- What are the decreasing subsequences of maximal length?

$$\langle 10, 9, 7, 4 \rangle$$

Theorem

Suppose $m, n \in \mathbb{N} - \{0\}$. A sequence of more than $m \cdot n$ real numbers must contain either an increasing subsequence of length at least $m + 1$, or a strictly decreasing subsequence of length at least $n + 1$.

PROOF.

$$r_1, r_2, \ldots, r_{m \cdot n+1}$$

For every $1 \leq i \leq m \cdot n + 1$, let

a_i :=length of longest increasing subseq. starting with r_i
d_i :=length of longest strictly decreasing subseq. starting with r_i

For example, if the sequence is $3, 5, 8, 10, 6, 1, 9, 2, 7, 4$ then

$a_2 = 3$ (for the subsequence $5, 8, 10$ or $5, 8, 9$)
$d_2 = 2$ (for the subsequence $5, 1$ or $5, 2$)

- We assume the theorem is false $\Rightarrow 1 \le a_i \le m$ and $1 \le d_i \le n$
  $\Rightarrow$ the pair (a_i, d_i) has $m \cdot n$ possible values.
- There are $m \cdot n + 1$ such pairs $\Rightarrow \exists i < j$ with $(a_i, d_i) = (a_j, d_j)$.
- If $i < j$ and $(a_i, d_i) = (a_j, d_j)$ then
  1. The maximum length of increasing subsequences starting from r_i and from r_j is a_i.
  2. The maximum length of strictly decreasing subsequences starting from r_i and from r_j is d_i.
- But this is impossible, because
  1. If $r_i \le r_j$ then there there is
  $$\underbrace{r_i \le \overbrace{r_j \le \ldots}^{\text{length } a_i}}_{\text{length } a_i+1}$$
  2. If $r_i > r_j$ then there is
  $$\underbrace{r_i > \overbrace{r_j > \ldots}^{\text{length } d_i}}_{\text{length } d_i+1}.$$

For every real number $x \in \mathbb{R}$ we define:

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.
- The fractional part of x:
  $\{x\} := x - \lfloor x \rfloor$

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.
- The fractional part of x:
  $\{x\} := x - \lfloor x \rfloor$
- An irrational number is a number that can not be obtained by dividing two integers.

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.
- The fractional part of x:
  $\{x\} := x - \lfloor x \rfloor$
- An irrational number is a number that can not be obtained by dividing two integers.
- Examples: $\pi = 3.14159265\ldots$, $e = 2.7182818\ldots$, etc.

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.
- The fractional part of x:
  $\{x\} := x - \lfloor x \rfloor$
- An irrational number is a number that can not be obtained by dividing two integers.
- Examples: $\pi = 3.14159265\ldots$, $e = 2.7182818\ldots$, etc.
- If α is an irrational number and $Q \in \mathbb{N} - \{0\}$, how close can we approximate α with a rational number $\frac{p}{q}$ when $1 \leq q \leq Q$?

For every real number $x \in \mathbb{R}$ we define:

- The floor of x:
  $\lfloor x \rfloor :=$ largest integer m satisfying $m \leq x$.
- The ceiling of x:
  $\lceil x \rceil :=$ smallest integer m satisfying $x \leq m$.
- The fractional part of x:
  $\{x\} := x - \lfloor x \rfloor$
- An irrational number is a number that can not be obtained by dividing two integers.
- Examples: $\pi = 3.14159265\ldots$, $e = 2.7182818\ldots$, etc.
- If α is an irrational number and $Q \in \mathbb{N} - \{0\}$, how close can we approximate α with a rational number $\frac{p}{q}$ when $1 \leq q \leq Q$?
  - How small can $\left|\alpha - \dfrac{p}{q}\right|$ become when $1 \leq q \leq Q$?

Theorem (Dirichlet's approximation theorem)

If α is an irrational number and Q a positive integer, then there exists a rational number p/q with $1 \le q \le Q$ such that

$$\left|\alpha - \frac{p}{q}\right| \le \frac{1}{q \cdot (Q+1)}.$$

PROOF. Divide $[0,1]$ into $Q+1$ subintervals of equal length:

$$\left[0, \frac{1}{Q+1}\right), \left[\frac{1}{Q+1}, \frac{2}{Q+1}\right), \dots, \left[\frac{Q}{Q+1}, 1\right]$$

and consider the $Q+2$ real numbers

$$r_1 = 0, r_2 = \{\alpha\}, \{2\alpha\}, \dots, r_{Q+1} = \{Q\alpha\}, r_{Q+2} = 1$$

- There are $Q+2$ objects in $Q+1$ intervals

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval
  $\Rightarrow |r_i - r_j| \leq \frac{1}{Q+1}$. Note that $(i,j) \neq (1, Q+2)$

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval
  $\Rightarrow |r_i - r_j| \leq \frac{1}{Q+1}$. Note that $(i,j) \neq (1, Q+2)$
  We note that

$$\begin{aligned} r_1 &= 0 \cdot \alpha - 0 \\ r_i &= (i-1) \cdot \alpha - \lfloor (i-1)\alpha \rfloor \quad \text{if } 2 \leq i \leq Q+1 \\ r_{Q+2} &= 0 \cdot \alpha - (-1) \end{aligned}$$

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval
  $\Rightarrow |r_i - r_j| \leq \frac{1}{Q+1}$. Note that $(i,j) \neq (1, Q+2)$
  We note that

$$\begin{array}{rcccl}
r_1 = & 0 & \cdot\alpha- & 0 & \\
r_i = & (i-1) & \cdot\alpha- & \lfloor (i-1)\alpha \rfloor & \text{if } 2 \leq i \leq Q+1 \\
r_{Q+2} = & 0 & \cdot\alpha- & (-1) &
\end{array}$$

  $\Rightarrow$ every r_i is $u_i \cdot \alpha - v_i$ with $u_i, v_i \in \mathbb{Z}$, and
  - if $i<j$ then $u_i = u_j$ only if $(i,j) = (1, Q+2)$.

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval
  $\Rightarrow |r_i - r_j| \leq \frac{1}{Q+1}$. Note that $(i,j) \neq (1, Q+2)$
  We note that

$$\begin{array}{rcccl} r_1 = & 0 & \cdot\alpha - & 0 & \\ r_i = & (i-1) & \cdot\alpha - & \lfloor (i-1)\alpha \rfloor & \text{if } 2 \leq i \leq Q+1 \\ r_{Q+2} = & 0 & \cdot\alpha - & (-1) & \end{array}$$

  $\Rightarrow$ every r_i is $u_i \cdot \alpha - v_i$ with $u_i, v_i \in \mathbb{Z}$, and
  - if $i<j$ then $u_i = u_j$ only if $(i,j) = (1, Q+2)$.

$$\Rightarrow |r_i - r_j| = |(u_i - u_j)\alpha - (v_i - v_j)| = \underbrace{|u_i - u_j|}_{q \in [1,Q]} \cdot \left|\alpha - \underbrace{\frac{v_i - v_j}{u_i - u_j}}_{\frac{p}{q}}\right| \leq \frac{1}{Q+1}.$$

- There are $Q+2$ objects in $Q+1$ intervals
  $\Rightarrow$ there is $i<j$ with r_i, r_j in same interval
  $\Rightarrow |r_i - r_j| \leq \frac{1}{Q+1}$. Note that $(i,j) \neq (1, Q+2)$
  We note that

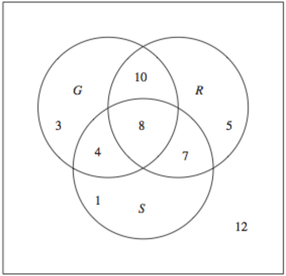
$$\begin{array}{rcccl} r_1 = & 0 & \cdot\alpha - & 0 & \\ r_i = & (i-1) & \cdot\alpha - & \lfloor (i-1)\alpha \rfloor & \text{if } 2 \leq i \leq Q+1 \\ r_{Q+2} = & 0 & \cdot\alpha - & (-1) & \end{array}$$

  $\Rightarrow$ every r_i is $u_i \cdot \alpha - v_i$ with $u_i, v_i \in \mathbb{Z}$, and
  - if $i<j$ then $u_i = u_j$ only if $(i,j) = (1, Q+2)$.

$$\Rightarrow |r_i - r_j| = |(u_i - u_j)\alpha - (v_i - v_j)| = \underbrace{|u_i - u_j|}_{q\in[1,Q]} \cdot \Big|\alpha - \underbrace{\frac{v_i - v_j}{u_i - u_j}}_{\frac{p}{q}}\Big| \leq \frac{1}{Q+1}.$$

- Thus $\left|\alpha - \dfrac{p}{q}\right| \leq \dfrac{1}{q \cdot (Q+1)}$.

- Suppose there are 50 beads in a drawer: 25 are glass, 30 are red, 20 are spherical, 18 are red glass, 12 are glass spheres, 15 are red spheres, and 8 are red glass spheres. How many beads are neither red, nor glass, nor spheres?
- ANSWER: use a Venn diagram with 3 overlapping sets: G of glass beads, R of red beads, and S of spherical beads.



OBSERVATION. $|G \cup R \cup S| =$
$|G| + |R| + |S| - |G \cap R| - |G \cap S| - |R \cap S| + |G \cap R \cap S|$.

Assumptions:

- N: a universal set
- $a_1, \ldots, a_r$: properties of the elements of set N
- $N(a_{i_1} a_{i_2} \ldots a_{i_m})$: the number of objects of N which have properties $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$ simultaneously.
- N_0: the number of objects having none of these properties.

Theorem (Principle of Inclusion and Exclusion)

$$N_0 = N - \sum_{i} N(a_i) + \sum_{i<j} N(a_i a_j) - \sum_{i<j<k} N(a_i a_j a_k) + \ldots + (-1)^m \sum_{i_1<\cdots<i_m} N(a_{i_1} \ldots a_{i_m}) + \ldots + (-1)^r N(a_1 a_2 \ldots a_r).$$

- $\varphi(n)$:= number of integers $1 \leq m < n$ with $\gcd(m, n) = 1$.
- Example: $\varphi(24) = 8$ because there are 8 integers between 1 and 23 that have no factor in common with 24: 1,5,7,11,13,17,19,23.
- $\varphi(n)$ is very important in number theory.
- $\varphi(n)$ can be computed using the principle of inclusion and exclusion:
  - Suppose $n = p_1^{n_1} \dots p_r^{n_r}$ where $p_1, \dots, p_r$ are distinct prime numbers, and $n_i > 0$ for $1 \leq i \leq r$.
  - Let a_i be the property "smaller than n and divisible by p_i" $(1 \leq i \leq r)$
  - $\Rightarrow \varphi(n) = N_0 =$
    $$n - \sum_i N(a_i) + \sum_{i<j} N(a_i a_j) + \ldots + (-1)^r N(a_1 \dots a_r).$$
  - $N(a_{i_1} \dots, a_{i_m})$ is the number of elements $< n$ divisible by $p_{i_1} \cdot \ldots \cdot p_{i_m} \Rightarrow N(a_{i_1} \dots a_{i_m}) = \dfrac{n}{p_{i_1} \cdot \ldots \cdot p_{i_m}}$.

$$\varphi(n) = n - \sum_{i} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} + \ldots + (-1)^n \frac{n}{p_1 p_2 \ldots p_r}$$
$$= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

- Example: $\varphi(24) = \varphi(2^3 \cdot 3) = 24 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 8.$

How many prime numbers are between 1 and n?

How many prime numbers are between 1 and n?

REMARK: If n is not prime, then $n = a \cdot b$ with $1 < a \leq b$ $\Rightarrow a^2 \leq n$, so $a \leq \sqrt{n}$ and n must be divisible by a prime number $p \leq \sqrt{n}$.

How many prime numbers are between 1 and n?

REMARK: If n is not prime, then $n = a \cdot b$ with $1 < a \leq b$ $\Rightarrow a^2 \leq n$, so $a \leq \sqrt{n}$ and n must be divisible by a prime number $p \leq \sqrt{n}$.

$\Rightarrow$ CRITERION to count the prime numbers $< n$:

How many prime numbers are between 1 and n?

REMARK: If n is not prime, then $n = a \cdot b$ with $1 < a \leq b$ $\Rightarrow a^2 \leq n$, so $a \leq \sqrt{n}$ and n must be divisible by a prime number $p \leq \sqrt{n}$.

$\Rightarrow$ CRITERION to count the prime numbers $< n$:

- Start with the set of integers $N = \{1, \ldots, n\}$ and count $N_0 =$ the number of elements left when multiples of prime numbers $p \leq \sqrt{n}$ are excluded from the set.

How many prime numbers are between 1 and n?

REMARK: If n is not prime, then $n = a \cdot b$ with $1 < a \leq b$ $\Rightarrow a^2 \leq n$, so $a \leq \sqrt{n}$ and n must be divisible by a prime number $p \leq \sqrt{n}$.

$\Rightarrow$ CRITERION to count the prime numbers $< n$:

- Start with the set of integers $N = \{1, \ldots, n\}$ and count $N_0 =$ the number of elements left when multiples of prime numbers $p \leq \sqrt{n}$ are excluded from the set.
- The number obtained is *not exactly what we want* because
  - we did not count the prime numbers $\leq \sqrt{n}$
  - we did count 1

How many prime numbers are between 1 and n?

REMARK: If n is not prime, then $n = a \cdot b$ with $1 < a \leq b$ $\Rightarrow a^2 \leq n$, so $a \leq \sqrt{n}$ and n must be divisible by a prime number $p \leq \sqrt{n}$.

$\Rightarrow$ CRITERION to count the prime numbers $< n$:

- Start with the set of integers $N = \{1, \ldots, n\}$ and count $N_0 =$ the number of elements left when multiples of prime numbers $p \leq \sqrt{n}$ are excluded from the set.
- The number obtained is *not exactly what we want* because
  - we did not count the prime numbers $\leq \sqrt{n}$
  - we did count 1
- The number we are looking for is

$$N_0 + r - 1$$

where r is the number of prime numbers $\leq \sqrt{n}$.

How many prime numbers are between 1 and 120?

How many prime numbers are between 1 and 120?

- The largest prime number $\leq \sqrt{120}$ is 7

How many prime numbers are between 1 and 120?

- The largest prime number $\leq \sqrt{120}$ is 7
  - Start with the universal set $N = \{n \in \mathbb{N} \mid 1 \leq n \leq 120\}$ and remove from N all elements divisible by a prime number ≤ 7. This means, we remove from N the elements with properties
    - $a_1 =$ "is divisible by $p_1 = 2$"
    - $a_2 =$ "is divisible by $p_2 = 3$"
    - $a_3 =$ "is divisible by $p_3 = 5$"
    - $a_4 =$ "is divisible by $p_4 = 7$"

    and obtain a set M with N_0 elements.

How many prime numbers are between 1 and 120?

- The largest prime number $\leq \sqrt{120}$ is 7
  - Start with the universal set $N = \{n \in \mathbb{N} \mid 1 \leq n \leq 120\}$ and remove from N all elements divisible by a prime number ≤ 7. This means, we remove from N the elements with properties
    - $a_1 =$ "is divisible by $p_1 = 2$"
    - $a_2 =$ "is divisible by $p_2 = 3$"
    - $a_3 =$ "is divisible by $p_3 = 5$"
    - $a_4 =$ "is divisible by $p_4 = 7$"

    and obtain a set M with N_0 elements.

Q: Is N_0 the number we want to compute?

How many prime numbers are between 1 and 120?

- The largest prime number $\leq \sqrt{120}$ is 7
  - Start with the universal set $N = \{n \in \mathbb{N} \mid 1 \leq n \leq 120\}$ and remove from N all elements divisible by a prime number ≤ 7. This means, we remove from N the elements with properties
    - $a_1 =$ "is divisible by $p_1 = 2$"
    - $a_2 =$ "is divisible by $p_2 = 3$"
    - $a_3 =$ "is divisible by $p_3 = 5$"
    - $a_4 =$ "is divisible by $p_4 = 7$"

    and obtain a set M with N_0 elements.

Q: Is N_0 the number we want to compute?

A: Almost correct, except that:

- M contains all prime numbers between 1 and 120, except $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.
- M contains 1, which is not prime.

How many prime numbers are between 1 and 120?

- The largest prime number $\leq \sqrt{120}$ is 7
  - Start with the universal set $N = \{n \in \mathbb{N} \mid 1 \leq n \leq 120\}$ and remove from N all elements divisible by a prime number ≤ 7. This means, we remove from N the elements with properties
    - $a_1 =$ "is divisible by $p_1 = 2$"
    - $a_2 =$ "is divisible by $p_2 = 3$"
    - $a_3 =$ "is divisible by $p_3 = 5$"
    - $a_4 =$ "is divisible by $p_4 = 7$"

    and obtain a set M with N_0 elements.

Q: Is N_0 the number we want to compute?

A: Almost correct, except that:

  - M contains all prime numbers between 1 and 120, except $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.
  - M contains 1, which is not prime.

- The number of prime numbers ≤ 120 is $N_0 + 4 - 1$.

How many prime numbers are between 1 and 120?

How many prime numbers are between 1 and 120?

- $N_0 = 120 - \sum_{i=1}^{4} N(a_i) + \sum_{i<j} N(a_i a_j) - \sum_{i<j<k} N(a_i a_j a_k) + N(a_1 a_2 a_3 a_4)$

How many prime numbers are between 1 and 120?

- $N_0 = 120 - \sum_{i=1}^{4} N(a_i) + \sum_{i<j} N(a_i a_j) - \sum_{i<j<k} N(a_i a_j a_k) + N(a_1 a_2 a_3 a_4)$
- Note that $N(a_{i_1} \dots a_{i_m}) = \left\lfloor \frac{120}{p_{i_1} \cdot \ldots \cdot p_{i_m}} \right\rfloor$ (why?)

  For example:
  - $N(a_1) = \lfloor 120/2 \rfloor = 60$, $N(a_2) = \lfloor 120/3 \rfloor = 40$,
    $N(a_3) = \lfloor 120/5 \rfloor = 24$, $N(a_4) = \lfloor 120/7 \rfloor = 17$
  - $N(a_1 a_2) = \lfloor 120/(2 \cdot 3) \rfloor = 20$, $N(a_1 a_3) = \lfloor 120/(2 \cdot 5) \rfloor = 12$,
    ...
  - $N(a_1 a_2 a_3 a_4) = \lfloor 120/(2 \cdot 3 \cdot 5 \cdot 7) \rfloor = \lfloor 120/210 \rfloor = 0$

How many prime numbers are between 1 and 120?

- $N_0 = 120 - \sum_{i=1}^{4} N(a_i) + \sum_{i<j} N(a_i a_j) - \sum_{i<j<k} N(a_i a_j a_k) + N(a_1 a_2 a_3 a_4)$
- Note that $N(a_{i_1} \dots a_{i_m}) = \left\lfloor \frac{120}{p_{i_1} \cdot \ldots \cdot p_{i_m}} \right\rfloor$ (why?)

  For example:
  - $N(a_1) = \lfloor 120/2 \rfloor = 60$, $N(a_2) = \lfloor 120/3 \rfloor = 40$,
    $N(a_3) = \lfloor 120/5 \rfloor = 24$, $N(a_4) = \lfloor 120/7 \rfloor = 17$
  - $N(a_1 a_2) = \lfloor 120/(2 \cdot 3) \rfloor = 20$, $N(a_1 a_3) = \lfloor 120/(2 \cdot 5) \rfloor = 12$,
    ...
  - $N(a_1 a_2 a_3 a_4) = \lfloor 120/(2 \cdot 3 \cdot 5 \cdot 7) \rfloor = \lfloor 120/210 \rfloor = 0$

$\Rightarrow N_0 = 120 - (60 + 40 + 24 + 17) + (20 + 12 + 8 + 8 + 5 + 3) - (4 + 2 + 1 + 1) + 0 = 27.$

How many prime numbers are between 1 and 120?

- $N_0 = 120 - \sum_{i=1}^{4} N(a_i) + \sum_{i<j} N(a_i a_j) - \sum_{i<j<k} N(a_i a_j a_k) + N(a_1 a_2 a_3 a_4)$
- Note that $N(a_{i_1} \dots a_{i_m}) = \left\lfloor \frac{120}{p_{i_1} \cdot \dots \cdot p_{i_m}} \right\rfloor$ (why?)
  For example:
  - $N(a_1) = \lfloor 120/2 \rfloor = 60$, $N(a_2) = \lfloor 120/3 \rfloor = 40$,
    $N(a_3) = \lfloor 120/5 \rfloor = 24$, $N(a_4) = \lfloor 120/7 \rfloor = 17$
  - $N(a_1 a_2) = \lfloor 120/(2 \cdot 3) \rfloor = 20$, $N(a_1 a_3) = \lfloor 120/(2 \cdot 5) \rfloor = 12$,
    ...
  - $N(a_1 a_2 a_3 a_4) = \lfloor 120/(2 \cdot 3 \cdot 5 \cdot 7) \rfloor = \lfloor 120/210 \rfloor = 0$

  $\Rightarrow N_0 = 120 - (60 + 40 + 24 + 17) + (20 + 12 + 8 + 8 + 5 + 3) - (4 + 2 + 1 + 1) + 0 = 27$.
- The number we are looking for is $27 + 4 - 1 = 30$

Bibliography

1. Chapter 2, Section 2.1: *Generating Permutations* of
   - S. Pemmaraju, S. Skiena. *Combinatorics and Graph Theory with Mathematica.* Cambridge University Press 2003.
2. Chapter 2, Sections 2.4 and 2.5 of
   - J. M. Harris, J. L. Hirst, M.J. Mossinghoff. *Combinatorics and Graph Theory*. Second Edition. Springer 2008.
3. Chapter 5 of
   - K. H. Rosen. *Discrete Mathematics and Its Applications.* Sixth Edition. McGraw Hill Higher Education. 2007.