Counting-Basics

Ngày 10 tháng 11 năm 2010

There are a few rules, or guidelines that help us count various collections. In many applications we can describe the objects as **tasks** and our goal is to count in how many different ways a task can be performed.

There are a few rules, or guidelines that help us count various collections. In many applications we can describe the objects as **tasks** and our goal is to count in how many different ways a task can be performed.

Example

There are 11 female students and 16 male students in our class. In how many ways can we choose a class leader?

There are a few rules, or guidelines that help us count various collections. In many applications we can describe the objects as **tasks** and our goal is to count in how many different ways a task can be performed.

Example

There are 11 female students and 16 male students in our class. In how many ways can we choose a class leader?

Answer

This task can be performed in 27 different ways.

There are a few rules, or guidelines that help us count various collections. In many applications we can describe the objects as **tasks** and our goal is to count in how many different ways a task can be performed.

Example

There are 11 female students and 16 male students in our class. In how many ways can we choose a class leader?

Answer

This task can be performed in 27 different ways.

Rule (The Sum Rule)

If a task can be performed either in m distinct ways or in k other distinct ways and both ways are mutually disjoint then there are $m + k$ distinct ways to perform the task.

Rule (The Product rule)

Suppose that a task has to be performed in two steps, where the first step can be performed in m different ways and the second step in k different ways, then there are $m \times k$ different ways to perform the task.

Rule (The Product rule)

Suppose that a task has to be performed in two steps, where the first step can be performed in m different ways and the second step in k different ways, then there are $m \times k$ different ways to perform the task.

Example

A motorbike license plate has the following format: x-Ay n where x is a two digit number, A is a letter followed by a single digit number y, and n is a four digit number. How many distinct license plates can be formed?

Rule (The Product rule)

Suppose that a task has to be performed in two steps, where the first step can be performed in m different ways and the second step in k different ways, then there are $m \times k$ different ways to perform the task.

Example

A motorbike license plate has the following format: x-Ay n where x is a two digit number, A is a letter followed by a single digit number y, and n is a four digit number. How many distinct license plates can be formed?

Answer

This task has 3 steps. The first step can be performed in 100 ways (assuming that 00 is O.K.). The second step can be performed in 260 ways (assuming 26 letters are available) and the third step can be performed in 10,000. So the total is 26,000,000.

Rule (The Product rule)

Suppose that a task has to be performed in two steps, where the first step can be performed in m different ways and the second step in k different ways, then there are $m \times k$ different ways to perform the task.

Example

A motorbike license plate has the following format: x-Ay n where x is a two digit number, A is a letter followed by a single digit number y, and n is a four digit number. How many distinct license plates can be formed?

Answer

This task has 3 steps. The first step can be performed in 100 ways (assuming that 00 is O.K.). The second step can be performed in 260 ways (assuming 26 letters are available) and the third step can be performed in 10,000. So the total is 26,000,000.

Rule (The Product rule)

Suppose that a task has to be performed in two steps, where the first step can be performed in m different ways and the second step in k different ways, then there are $m \times k$ different ways to perform the task.

Example

A motorbike license plate has the following format: x-Ay n where x is a two digit number, A is a letter followed by a single digit number y, and n is a four digit number. How many distinct license plates can be formed?

Answer

This task has 3 steps. The first step can be performed in 100 ways (assuming that 00 is O.K.). The second step can be performed in 260 ways (assuming 26 letters are available) and the third step can be performed in 10,000. So the total is 26,000,000. Are there only 26,000,000 motorbikes in Hanoi?

More product rule examples

Question

How many distinct functions $f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \rightarrow \{1, 2, 3, 4\}$ *are there?*

More product rule examples

Question

How many distinct functions
$f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \to \{1, 2, 3, 4\}$ *are there?*

Answer

Each function is built in 10 steps: choose a value for
$f(1), f(2), \ldots, f(0)$*.*
Each step can be performed in 4 *different ways.*
So the number of functions is:

More product rule examples

Question

How many distinct functions
$f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \to \{1, 2, 3, 4\}$ *are there?*

Answer

Each function is built in 10 steps: choose a value for
$f(1), f(2), \ldots, f(0)$.
Each step can be performed in 4 *different ways.*
So the number of functions is:

More product rule examples

Question

How many distinct functions $f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \to \{1, 2, 3, 4\}$ *are there?*

Answer

Each function is built in 10 steps: choose a value for $f(1), f(2), \dots, f(0)$.
Each step can be performed in 4 *different ways.*
So the number of functions is: 4^{10}.

Question

How many $1-1$ *functions* $f : \{a, b, c\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *are there?*

More product rule examples

Question

How many distinct functions
$f : \{1,2,3,4,5,6,7,8,9,0\} \to \{1,2,3,4\}$ *are there?*

Answer

Each function is built in 10 steps: choose a value for $f(1), f(2), \ldots, f(0)$.
Each step can be performed in 4 *different ways.*
So the number of functions is: 4^{10}.

Question

How many $1-1$ *functions*
$f : \{a,b,c\} \to \{0,1,2,3,4,5,6,7,8,9\}$ *are there?*

More product rule examples

Question

How many distinct functions
$f : \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \to \{1, 2, 3, 4\}$ *are there?*

Answer

Each function is built in 10 steps: choose a value for
$f(1), f(2), \ldots, f(0)$*.*
Each step can be performed in 4 *different ways.*
So the number of functions is: 4^{10}.

Question

How many $1-1$ *functions*
$f : \{a, b, c\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *are there?*

Answer: Each function requires 3 steps: select a value for $f(a)$ then $f(b)$ and $f(c)$. $f(a)$ can be chosen in 10 different ways, $f(b)$ in 9 and $f(c)$ in 8. So the total number of functions is 720.

The Inclusion-Exclusion Principle

Rule

If a task can be performed either in m distinct ways or in k other distinct ways and there are n ways common to both then there are $m + k - n$ distinct ways to perform the task.

The Inclusion-Exclusion Principle

Rule

If a task can be performed either in m distinct ways or in k other distinct ways and there are n ways common to both then there are $m + k - n$ distinct ways to perform the task.

Example

How many bit strings of length 10 start with a 1 **or** *end with 10?*

The Inclusion-Exclusion Principle

Rule

If a task can be performed either in m distinct ways or in k other distinct ways and there are n ways common to both then there are $m + k - n$ distinct ways to perform the task.

Example

How many bit strings of length 10 start with a 1 **or** *end with 10?*

Answer

There are 2^9 bit strings that begin with a 1. There are 2^8 bit strings that end with 10. There are 2^7 bit strings that start with 1 and end with 10. Therefore the number of bitstrings of length 10 that start with a 1 or end with 10 is $2^9 + 2^8 - 2^7$.

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

1. *Let* A_{1729} *denote this set.*

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

1. *Let* A_{1729} *denote this set.*
2. *We first need to find the prime factors of* 1729.

Inclusion-Exclusion Example

Question

How many integers < 1729 are relatively prime to 1729?

Answer

1. *Let A_{1729} denote this set.*
2. *We first need to find the prime factors of 1729.*
3. $1729 = 7 \cdot 13 \cdot 19$.

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

1. *Let* A_{1729} *denote this set.*
2. *We first need to find the prime factors of* 1729.
3. $1729 = 7 \cdot 13 \cdot 19$.
4. *The following sets include all numbers that are not relatively prime to* 1729*:* $A = \{7, 14, \ldots, 1722\}$, $B = \{13, 26, \ldots, 1716\}$, $C = \{19, 38, \ldots 1710\}$

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

1. *Let* A_{1729} *denote this set.*
2. *We first need to find the prime factors of* 1729.
3. $1729 = 7 \cdot 13 \cdot 19$.
4. *The following sets include all numbers that are not relatively prime to* 1729*:* $A = \{7, 14, \ldots, 1722\}$, $B = \{13, 26, \ldots, 1716\}$, $C = \{19, 38, \ldots 1710\}$
5. *The set of numbers that are not relatively prime to* A_{1729} *is* $A \cup B \cup C$ *.*

Inclusion-Exclusion Example

Question

How many integers < 1729 *are relatively prime to* 1729*?*

Answer

1. *Let* A_{1729} *denote this set.*
2. *We first need to find the prime factors of* 1729.
3. $1729 = 7 \cdot 13 \cdot 19$.
4. *The following sets include all numbers that are not relatively prime to* 1729*:* $A = \{7, 14, \ldots, 1722\}$, $B = \{13, 26, \ldots, 1716\}$, $C = \{19, 38, \ldots 1710\}$
5. *The set of numbers that are not relatively prime to* A_{1729} *is* $A \cup B \cup C$.
6. $|A_{1729}| = 1728 - \frac{1729}{7} - \frac{1729}{13} - \frac{1729}{19} + \frac{1729}{7 \cdot 13} + \frac{1729}{7c19} + \frac{1729}{13 \cdot 19} = 1296.$

Theorem

For a finite family of finite sets $\{A_1, A_2, \ldots A_n\}$ *we have:*
$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\ldots,n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$.

We shall give three different proofs of this theorem, one in full detail and two hints.

The Inclusion-Exclusion General Principle

Theorem

For a finite family of finite sets $\{A_1, A_2, \dots A_n\}$ *we have:*
$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\dots,n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$.

We shall give three different proofs of this theorem, one in full detail and two hints.

Chứng minh.

The Inclusion-Exclusion General Principle

Theorem

For a finite family of finite sets $\{A_1, A_2, \ldots A_n\}$ *we have:*
$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\ldots,n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$.

We shall give three different proofs of this theorem, one in full detail and two hints.

Chứng minh.

1. $\forall x \in \cup_{i=1}^{n} A_i$ x contributes 1 to $|\cup_{i=1}^{n} A_i|$.

The Inclusion-Exclusion General Principle

Theorem

For a finite family of finite sets $\{A_1, A_2, \ldots A_n\}$ *we have:*
$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\ldots,n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$.

We shall give three different proofs of this theorem, one in full detail and two hints.

Chứng minh.

1. $\forall x \in \cup_{i=1}^{n} A_i$ x contributes 1 to $|\cup_{i=1}^{n} A_i|$.
2. Let $x \in \cap_{j=1}^{k} A_{i_j}$.

The Inclusion-Exclusion General Principle

Theorem

For a finite family of finite sets $\{A_1, A_2, \dots A_n\}$ *we have:*
$|\cup_{i=1}^{n} A_i| = \sum_{\emptyset \neq I \subset \{1,2,\dots,n\}} (-1)^{|I|-1} |\cap_{i \in I} A_i|$.

We shall give three different proofs of this theorem, one in full detail and two hints.

Chứng minh.

1. $\forall x \in \cup_{i=1}^{n} A_i$ x contributes 1 to $|\cup_{i=1}^{n} A_i|$.
2. Let $x \in \cap_{j=1}^{k} A_{i_j}$.
3. Since x belongs to every set A_{i_j}, it contributes:

$$\sum_{\emptyset \neq I \subset \{1,2,\dots k\}} (-1)^{|I|-1} |\cap_{\mathrm{j} \in I} A_{i_j}| = \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} = 1$$

(by the binomial theorem.)

Remark

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.
2. *We can use induction to prove the inclusion-exclusion principle, left as an exercise.*

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.
2. *We can use induction to prove the inclusion-exclusion principle, left as an exercise.*
3. *We can also use the characteristic functions of the sets* A_i *with the following identity:*

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.
2. *We can use induction to prove the inclusion-exclusion principle, left as an exercise.*
3. *We can also use the characteristic functions of the sets* A_i *with the following identity:*

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.
2. *We can use induction to prove the inclusion-exclusion principle, left as an exercise.*
3. *We can also use the characteristic functions of the sets* A_i *with the following identity:*

Remark

1. *For two subsets we already know that* $|A \cup B| = |A| + |B| - |A \cap B|$.
2. *We can use induction to prove the inclusion-exclusion principle, left as an exercise.*
3. *We can also use the characteristic functions of the sets* A_i *with the following identity:*

$$\prod_{i=1}^{n}(1 + x_i) = \sum_{A \subset \{1,2,\ldots,n\}} \Big(\prod_{i \in A} x_i\Big)$$

Two counting problems "saved" by the inclusion-exclusion principle

Problem 1. n persons check their coats before entering the theatre. At the end of the play, each selects randomly a coat. In how many ways can the selection be done so that no person gets his coat.

Two counting problems "saved" by the inclusion-exclusion principle

Problem 1. n persons check their coats before entering the theatre. At the end of the play, each selects randomly a coat. In how many ways can the selection be done so that no person gets his coat.
An aletrnative formulation using "Tiếng Mathematics:" how many $1-1$ functions $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ are such that $f(i) \neq i$.

Also known as *d*erangements.

Two counting problems "saved" by the inclusion-exclusion principle

Problem 1. n persons check their coats before entering the theatre. At the end of the play, each selects randomly a coat. In how many ways can the selection be done so that no person gets his coat.
An aletrnative formulation using "Tiếng Mathematics:" how many $1-1$ functions $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ are such that $f(i) \neq i$.

Also known as *d*erangements.

We shall count the number of permutations for which $f(i) = i$ for some i.

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$
4. And generally, $|\cap_{j=1}^{k} A_{i_j}| = (n-k)!$.

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$
4. And generally, $|\cap_{j=1}^{k} A_{i_j}| = (n-k)!$.
5. Applying the inclusion-exclusion theorem we get:

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$
4. And generally, $|\cap_{j=1}^{k} A_{i_j}| = (n-k)!$.
5. Applying the inclusion-exclusion theorem we get:

Continued

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$
4. And generally, $| \cap_{j=1}^{k} A_{i_j}| = (n-k)!$.
5. Applying the inclusion-exclusion theorem we get:

$$| \cup_{i=1}^{n} A_i| = \sum_{j=1}^{n} (-1)^{(j-1)} \binom{n}{j} (n-j)! = \sum_{j=1}^{n} (-1)^{j-1} \frac{n!}{j!}$$

So the number of derangements is:

1. Let A_i be the set of permutations for which $f(i) = i$. To apply the inclusion-exclusion theorem we need to find the size of the intersections $\cap_{i \in J} A_i$.
2. Clearly, $|A_i| = (n-1)!$.
3. $|A_i \cap A_j| = (n-2)!$
4. And generally, $| \cap_{j=1}^{k} A_{i_j}| = (n-k)!$.
5. Applying the inclusion-exclusion theorem we get:

$$| \cup_{i=1}^{n} A_i| = \sum_{j=1}^{n} (-1)^{(j-1)} \binom{n}{j} (n-j)! = \sum_{j=1}^{n} (-1)^{j-1} \frac{n!}{j!}$$

So the number of derangements is:

$$D_n = n! - \sum_{j=1}^{n} (-1)^{j-1} \cdot \frac{n!}{j!} = n! \cdot \sum_{j=0}^{n} (-1)^{j} \frac{1}{j!}$$

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m,n) = 1\}|$.

Example

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when p is a prime number.*

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when* p *is a prime number.*
2. *If* $n = p^k$ *then* $\phi(n) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when* p *is a prime number.*
2. *If* $n = p^k$ *then* $\phi(n) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$
3. *If* $n = p \cdot q$, p, q *distinct primes then* $\phi(p \cdot q) = (p - 1)(q - 1)$.

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when p is a prime number.*
2. *If* $n = p^k$ *then* $\phi(n) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$
3. *If* $n = p \cdot q$, p, q *distinct primes then* $\phi(p \cdot q) = (p - 1)(q - 1)$.

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when p is a prime number.*
2. *If* $n = p^k$ *then* $\phi(n) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$
3. *If* $n = p \cdot q,\ p, q$ *distinct primes then* $\phi(p \cdot q) = (p - 1)(q - 1)$.

Any integer n has a prime factorization: $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k}$.

Euler's function $\phi(n)$

Euler's function is very important in many applications, in particular in computer security applications.

Definition

Euler's function: $\phi(n) = |\{m \mid 0 < m < n \wedge GCD(m, n) = 1\}|$.

Example

1. $\phi(p) = p - 1$ *when p is a prime number.*
2. *If* $n = p^k$ *then* $\phi(n) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$
3. *If* $n = p \cdot q,\ p, q$ *distinct primes then* $\phi(p \cdot q) = (p - 1)(q - 1)$.

Any integer n has a prime factorization: $n = p_1^{r_1} \cdot p_2^{r_2} \ldots p_k^{r_k}$.

Our goal is to calculate $\phi(n)$.

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Chứng minh.

Let $A_i = \{s |\ 1 < s < n,\ p_i | s\}$. Then:

1. $|A_i| = \frac{n}{p_i}$

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Chứng minh.

Let $A_i = \{s | \ 1 < s < n, \ p_i | s\}$. Then:

1. $|A_i| = \frac{n}{p_i}$

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Chứng minh.

Let $A_i = \{s | \ 1 < s < n, \ p_i | s\}$. Then:

$$1. \ |A_i| = \frac{n}{p_i} \qquad 2. \ \phi(n) = n - |\cup_{i=1}^{k} A_i|$$

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Chứng minh.

Let $A_i = \{s |\ 1 < s < n,\ p_i | s\}$. Then:

$$1.\ |A_i| = \frac{n}{p_i} \qquad 2.\ \phi(n) = n - |\cup_{i=1}^{k} A_i|$$

Recall that:

$$|\cup_{i=1}^{k} A_i| = \sum_{\substack{I \subset \{1,2,\dots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} |\cap_{i \in I} A_i|.$$

Calculating $\phi(n)$

Theorem

For $n = p_1^{r_1} \cdot p_2^{r_2} \dots p_k^{r_k} \quad \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

Chứng minh.

Let $A_i = \{s|\ 1 < s < n,\ p_i|s\}$. Then:

$$1.\ |A_i| = \frac{n}{p_i} \qquad 2.\ \phi(n) = n - |\cup_{i=1}^{k} A_i|$$

Recall that:

$$|\cup_{i=1}^{k} A_i| = \sum_{\substack{I \subset \{1,2,\dots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} |\cap_{i \in I} A_i|.$$

$A_i \cap A_j$ is the set of all integers $\leq n$ that are divisible by p_i *and* p_j that is divisible by $p_i \cdot p_j$. It follows that $|A_i \cap A_j| = \frac{n}{p_i p_j}$. $\square$

continued.

Similarly,

$$|\cap_{i\in I\subset\{1,2,\ldots,k\}} A_i| = n/\prod_{i\in I} p_i$$

Hence:

$$\phi(n) = n \;\; - \sum_{\substack{I\subset\{1,2,\ldots,k\}\\ I\neq\emptyset}} (-1)^{|I|-1}|\cap_{i\in I} A_i| =$$

n - $\sum_{\substack{I\subset\{1,2,\ldots,k\}\\ I\neq\emptyset}}(-1)^{|I|-1}(n/\prod_{i\in I} p_i) = n(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_k})$ □

continued.

Similarly,

$$|\cap_{i \in I \subset \{1,2,\ldots,k\}} A_i| = n / \prod_{i \in I} p_i$$

Hence:

$$\phi(n) = n \;\; - \sum_{\substack{I \subset \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} |\cap_{i \in I} A_i| =$$

n - $\sum_{\substack{I \subset \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} (n / \prod_{i \in I} p_i) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$ □

continued.

Similarly,

$$|\cap_{i \in I \subset \{1,2,\ldots,k\}} A_i| = n / \prod_{i \in I} p_i$$

Hence:

$$\phi(n) = n \ \ - \sum_{\substack{I \subset \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} |\cap_{i \in I} A_i| =$$

n - $\sum_{\substack{I \subset \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{|I|-1} (n / \prod_{i \in I} p_i) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$ $\square$

The last equality is an instance of the general useful identity that embodies the Sum-Product rule:

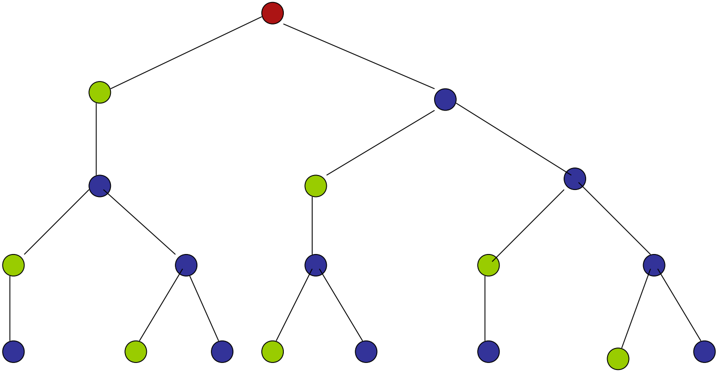
$$\prod_{i=1}^{n} (1 + x_i) = \sum_{A \subset \{1,2,\ldots,n\}} (\prod_{i \in A} x_i)$$

Tree Diagrams

How many bead strings of length four, composed of green and blue beads without two consecutive green beads can be constructed?

Tree Diagrams

How many bead strings of length four, composed of green and blue beads without two consecutive green beads can be constructed?



Rule (Pigeonhole Principle)

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k + 1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k+1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*
2. *If n pigeons are placed in k pigoenholes then there is at least one hole with $\lceil \frac{n}{k} \rceil$ pigeons.*

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k+1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*
2. *If n pigeons are placed in k pigoenholes then there is at least one hole with $\lceil \frac{n}{k} \rceil$ pigeons.*
3. *If n pigeons are placed in n pigeonholes and no hole is empty then every hole holds exactly one pigeon.*

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k+1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*
2. *If n pigeons are placed in k pigoenholes then there is at least one hole with $\lceil \frac{n}{k} \rceil$ pigeons.*
3. *If n pigeons are placed in n pigeonholes and no hole is empty then every hole holds exactly one pigeon.*

Remark

The four rules are simple, self explanatory and obvious, Yet they exhibit a surprising power to solve some intricate counting problems.

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k+1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*
2. *If n pigeons are placed in k pigoenholes then there is at least one hole with $\lceil \frac{n}{k} \rceil$ pigeons.*
3. *If n pigeons are placed in n pigeonholes and no hole is empty then every hole holds exactly one pigeon.*

Remark

The four rules are simple, self explanatory and obvious, Yet they exhibit a surprising power to solve some intricate counting problems.

The Pigeonhole Principle

Rule (Pigeonhole Principle)

1. *If $k+1$ pigeons are placed in k pigeonholes then at least one hole contains more than one pigeon.*
2. *If n pigeons are placed in k pigoenholes then there is at least one hole with $\lceil \frac{n}{k} \rceil$ pigeons.*
3. *If n pigeons are placed in n pigeonholes and no hole is empty then every hole holds exactly one pigeon.*

Remark

The four rules are simple, self explanatory and obvious, Yet they exhibit a surprising power to solve some intricate counting problems.
We shall next visit some examples.

Example

In a previous exercise you were asked to produce an integer n *and find an integer* k *such that* $n \cdot k = 111\ldots1$.
Some had the idea to produce the numbers $111\ldots1$, *check whether they are divisible by* n *and if so, find* k.

Example

In a previous exercise you were asked to produce an integer n *and find an integer* k *such that* $n \cdot k = 111\ldots1$.
Some had the idea to produce the numbers $111\ldots1$, *check whether they are divisible by* n *and if so, find* k.

Example

In a previous exercise you were asked to produce an integer n and find an integer k such that $n \cdot k = 111\ldots1$.
Some had the idea to produce the numbers $111\ldots1$, check whether they are divisible by n and if so, find k.
Did any one bother to ask whether the program will ever stop?

Example

In a previous exercise you were asked to produce an integer n *and find an integer* k *such that* $n \cdot k = 111\ldots1$.
Some had the idea to produce the numbers $111\ldots1$, *check whether they are divisible by* n *and if so, find* k.
Did any one bother to ask whether the program will ever stop?

Theorem

For any odd positive integer n *that is relatively prime to* 5 *one can find an integer* k *such that* $n \cdot k = 11\ldots1$.

Chứng minh.

□

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).
3. Now place the integer $k = 1^{\{j\}}$ mod n *in* h_k.

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).
3. Now place the integer $k = 1^{\{j\}}$ mod n *in* h_k.
4. If k is placed in h_0 then n divides $1^{\{j\}}$.

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).
3. Now place the integer $k = 1^{\{j\}}$ mod n *in* h_k.
4. If k is placed in h_0 then n divides $1^{\{j\}}$.
5. Else if $j = n$ one hole will have to contain two pigeons.

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).
3. Now place the integer $k = 1^{\{j\}} \bmod n$ *in* h_k.
4. If k is placed in h_0 then n divides $1^{\{j\}}$.
5. Else if $j = n$ one hole will have to contain two pigeons.
6. But this means that n divides $1^{\{j\}} - 1^{\{m\}} = 11\ldots10\ldots0$.

$\square$

Chứng minh.

1. Let $h_0, h_1, \ldots, h_{n-1}$ be n pigeonholes.
2. Let $1^{\{j\}} = 11\ldots1$ (j-ones).
3. Now place the integer $k = 1^{\{j\}} \bmod n$ *in* h_k.
4. If k is placed in h_0 then n divides $1^{\{j\}}$.
5. Else if $j = n$ one hole will have to contain two pigeons.
6. But this means that n divides $1^{\{j\}} - 1^{\{m\}} = 11\ldots10\ldots0$.
7. Since n is odd, and $GCD(n, 5) = 1$ we conclude that $1^{\{j-m\}}$ is a multiple of n

$\square$

The Chinese Reamainder theorem

Theorem

If $a_1, a_2, \ldots, a_k$ *are relatively prime, and* $0 \leq m_i < a_i$ *then there is a unique integer* $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ *such that* $m \bmod a_i = m_i$.

Theorem

If $a_1, a_2, \ldots, a_k$ are relatively prime, and $0 \leq m_i < a_i$ then there is a unique integer $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $m \bmod a_i = m_i$.

Chứng minh.

$\square$

The Chinese Reamainder theorem

Theorem

If $a_1, a_2, \ldots, a_k$ are relatively prime, and $0 \leq m_i < a_i$ then there is a unique integer $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $m \bmod a_i = m_i$.

Chứng minh.

1. Since a_i are relatively prime we can find integers b_i such that:

$\square$

The Chinese Reamainder theorem

Theorem

If $a_1, a_2, \ldots, a_k$ are relatively prime, and $0 \leq m_i < a_i$ then there is a unique integer $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $m \bmod a_i = m_i$.

Chứng minh.

1. Since a_i are relatively prime we can find integers b_i such that:
   - $b_i \bmod a_i = 1, \quad b_i \bmod a_j = 0$ *for* $i \neq j$.

$\square$

The Chinese Reamainder theorem

Theorem

If $a_1, a_2, \ldots, a_k$ are relatively prime, and $0 \leq m_i < a_i$ then there is a unique integer $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $m \bmod a_i = m_i$.

Chứng minh.

1. Since a_i are relatively prime we can find integers b_i such that:
   - $b_i \bmod a_i = 1, \quad b_i \bmod a_j = 0$ *for* $i \neq j$.
2. It is easy to check that the integer $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$ satisfies the relations: $s \bmod a_i = m_i$.

□

The Chinese Reamainder theorem

Theorem

If $a_1, a_2, \ldots, a_k$ are relatively prime, and $0 \leq m_i < a_i$ then there is a unique integer $m < M = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $m \bmod a_i = m_i$.

Chứng minh.

1. Since a_i are relatively prime we can find integers b_i such that:
   - $b_i \bmod a_i = 1, \quad b_i \bmod a_j = 0$ *for* $i \neq j$.
2. It is easy to check that the integer $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$ satisfies the relations: $s \bmod a_i = m_i$.
3. It remains to prove that s is unique.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M-1$.

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M - 1$.
2. There are M distinct k-tuples $m_1, m_2, \ldots, m_k,\ 0 \leq m_i < a_i$.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M-1$.
2. There are M distinct k-tuples $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$.
3. We place the k-tuple $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$ in h_s where $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M-1$.
2. There are M distinct k-tuples $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$.
3. We place the k-tuple $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$ in h_s where $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$.
4. Each integer $t < M$ produces a k-tuple $t_i = t \bmod a_i, i = 1, \ldots, k$ that will be placed in h_t.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M-1$.
2. There are M distinct k-tuples $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$.
3. We place the k-tuple $m_1, m_2, \ldots, m_k,\ 0 \le m_i < a_i$ in h_s where $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$.
4. Each integer $t < M$ produces a k-tuple $t_i = t \bmod a_i, i = 1, \ldots, k$ that will be placed in h_t.
5. Each hole contains a $k-tuple$. The number of k-tuples is equal to the number of holes.

$\square$

CRT-continued.

To prove uniqueness we use the pigeonhole principle.

1. Start with M holes numbered $0, 1, \ldots, M-1$.
2. There are M distinct k-tuples $m_1, m_2, \ldots, m_k,\ 0 \leq m_i < a_i$.
3. We place the k-tuple $m_1, m_2, \ldots, m_k,\ 0 \leq m_i < a_i$ in h_s where $s = (\sum_{i=1}^{k} m_i \cdot b_i) \bmod M$.
4. Each integer $t < M$ produces a k-tuple $t_i = t \bmod a_i, i = 1, \ldots, k$ that will be placed in h_t.
5. Each hole contains a $k - tuple$. The number of k-tuples is equal to the number of holes.
6. Conclusion: each hole contains exactly one item, or the uniqueness is established.

$\square$

Two more examples

Question (Example number 1)

In the ASEAN Cầu lông championship held in Hanoi, Linh won first place. The championship lasted 21 days. Linh played 35 matches, playing at least one match every day. Prove that there is a span of consecutive days in which Linh played exactly 6 matches.

The proof.

$\square$

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.

□

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.

$\square$

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.

$\square$

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.
4. x_i is also monotonically increasing and $x_{21} = 41$.

□

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.
4. x_i is also monotonically increasing and $x_{21} = 41$.
5. $\{m_i\}$ and $\{x_i\}$ together have 42 integers.

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.
4. x_i is also monotonically increasing and $x_{21} = 41$.
5. $\{m_i\}$ and $\{x_i\}$ together have 42 integers.
6. But the largest integer is 41, so at least one integer must appear twice.

□

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.
4. x_i is also monotonically increasing and $x_{21} = 41$.
5. $\{m_i\}$ and $\{x_i\}$ together have 42 integers.
6. But the largest integer is 41, so at least one integer must appear twice.
7. Since $m_i < m_j, \ and \ x_i < x_j \ if \ i < j$ we must have $m_i = x_j$ for some i and j.

$\square$

The proof.

1. Let m_i denote the total number of matches Linh played by the end of day number i.
2. This means that m_i is a monotonically increasing sequence and $m_{21} = 35$.
3. Let $x_i = m_i + 6$.
4. x_i is also monotonically increasing and $x_{21} = 41$.
5. $\{m_i\}$ and $\{x_i\}$ together have 42 integers.
6. But the largest integer is 41, so at least one integer must appear twice.
7. Since $m_i < m_j, \; and \; x_i < x_j \; if \; i < j$ we must have $m_i = x_j$ for some i and j.
8. But this means that between days j and i Linh played exactly 6 matches.

$\square$

Second example

Question

To commemerate Vua Le's defeat of the Chinese invaders, he decided to mint 11 commemerative gold coins. He gave a large amount of gold to a jeweler.
When the jeweler returned the coins, Vua Le suspected that the jeweler stole some gold and replaced it with cheaper metals. Vua Le, knew that the jeweler will not dare to tinker with more than one coin. The only way to identify the fake coin is to weigh coins on a balanced scale.

Second example

Question

To commemerate Vua Le's defeat of the Chinese invaders, he decided to mint 11 commemerative gold coins. He gave a large amount of gold to a jeweler.
When the jeweler returned the coins, Vua Le suspected that the jeweler stole some gold and replaced it with cheaper metals.
Vua Le, knew that the jeweler will not dare to tinker with more than one coin. The only way to identify the fake coin is to weigh coins on a balanced scale.

Second example

Question

To commemerate Vua Le's defeat of the Chinese invaders, he decided to mint 11 commemerative gold coins. He gave a large amount of gold to a jeweler.
When the jeweler returned the coins, Vua Le suspected that the jeweler stole some gold and replaced it with cheaper metals. Vua Le, knew that the jeweler will not dare to tinker with more than one coin. The only way to identify the fake coin is to weigh coins on a balanced scale.

Vua Le decided to test the intelligence of his chief adviser. He ordered him to design a weighing scheme to detect the fake coin, decide whether it is heavier or lighter by using no more than three weighings.

Second example

Question

To commemerate Vua Le's defeat of the Chinese invaders, he decided to mint 11 commemerative gold coins. He gave a large amount of gold to a jeweler.
When the jeweler returned the coins, Vua Le suspected that the jeweler stole some gold and replaced it with cheaper metals. Vua Le, knew that the jeweler will not dare to tinker with more than one coin. The only way to identify the fake coin is to weigh coins on a balanced scale.

Vua Le decided to test the intelligence of his chief adviser. He ordered him to design a weighing scheme to detect the fake coin, decide whether it is heavier or lighter by using no more than three weighings.

It is your mission to help the adviser by designing the weighing scheme.