R3.09

Cryptographie et sécurité

Le bon exemple, René MAGRITTE (1898-1967)

Congruence

Définition

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x \mathfrak{R} y$ si $\exists k \in \mathbb{Z}\ y - x = kn$

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x \mathfrak{R} y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x \mathfrak{R} y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x \mathfrak{R} y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x \mathfrak{R} y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.
Remarque : si $n = 0$

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x\mathfrak{R}y$ si $\exists k \in \mathbb{Z}$ $y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.
Remarque : si $n = 0$ alors $x\mathfrak{R}y$ s'écrit $x = y$.

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x\mathfrak{R}y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.
Remarque : si $n = 0$ alors $x\mathfrak{R}y$ s'écrit $x = y$.
Il s'agit de l'égalité $=$.

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x\mathfrak{R}y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.
Remarque : si $n = 0$ alors $x\mathfrak{R}y$ s'écrit $x = y$.
Il s'agit de l'égalité $=$.

Relation d'équivalence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Congruence

Définition

Soit $n \in \mathbb{Z}$. On définit $\mathfrak{R}$ sur $\mathbb{Z}$ par :
$x\mathfrak{R}y$ si $\exists k \in \mathbb{Z}\ y - x = kn$ (congruence modulo n).
$y - x$ est un multiple de n.
n divise $y - x$: $n \mid y - x$.
Remarque : si $n = 0$ alors $x\mathfrak{R}y$ s'écrit $x = y$.
Il s'agit de l'égalité $=$.

Relation d'équivalence

La congruence modulo n est une relation d'équivalence.

Congruence

Classes d'équivalence

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$

$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$
$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$
Exemple : $\overline{0} = \{0 + kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$
$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$
Exemple : $\overline{0} = \{0 + kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$

Remarques

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$
$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$
Exemple : $\overline{0} = \{0 + kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$

Remarques

$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$
$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$
Exemple : $\overline{0} = \{0 + kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$

Remarques

$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$
$\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\} = \{\overline{0}\}$

Congruence

Classes d'équivalence

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x},\ x \in \mathbb{Z}\}$
$\overline{x} = \{x + kn,\ k \in \mathbb{Z}\}$
Exemple : $\overline{0} = \{0 + kn,\ k \in \mathbb{Z}\} = n\mathbb{Z}$

Remarques

$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$
$\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\} = \{\overline{0}\}$
$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(-n)\mathbb{Z}$

Congruence

Théorème

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Théorème

Deux entiers a et b sont congrus entre eux modulo un entier n non nul si et seulement s'ils ont le même reste dans la division euclidienne par n.

Congruence

Théorème

Deux entiers a et b sont congrus entre eux modulo un entier n non nul si et seulement s'ils ont le même reste dans la division euclidienne par n.

Corollaire

Congruence

Théorème

Deux entiers a et b sont congrus entre eux modulo un entier n non nul si et seulement s'ils ont le même reste dans la division euclidienne par n.

Corollaire

Soit $n > 0$.

Congruence

Théorème

Deux entiers a et b sont congrus entre eux modulo un entier n non nul si et seulement s'ils ont le même reste dans la division euclidienne par n.

Corollaire

Soit $n > 0$.
L'ensemble des classes d'équivalence modulo n est
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$.

Congruence

Théorème

Deux entiers a et b sont congrus entre eux modulo un entier n non nul si et seulement s'ils ont le même reste dans la division euclidienne par n.

Corollaire

Soit $n > 0$.
L'ensemble des classes d'équivalence modulo n est
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$.
On dit que les nombres $(0, 1, ..., n-1)$ constituent un système de représentants de la congruence modulo n.

Congruence

Démonstration

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

R3.09 Cryptographie et sécurité

Département Informatique

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$
   et donc $r_a - r_b = kn$.

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$
   et donc $r_a - r_b = kn$.
   Or $-n < r_a - r_b < n$.

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$
   et donc $r_a - r_b = kn$.
   Or $-n < r_a - r_b < n$. D'où $r_a - r_b = 0$

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$
   et donc $r_a - r_b = kn$.
   Or $-n < r_a - r_b < n$. D'où $r_a - r_b = 0$
   et donc $r_a = r_b$.

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$ et donc $r_a - r_b = kn$. Or $-n < r_a - r_b < n$. D'où $r_a - r_b = 0$ et donc $r_a = r_b$.
2. Si $a = a'n + r$ et $b = b'n + r$ $(0 \leq r < n)$ alors $a - b = (a' - b')n$

Congruence

Démonstration

Soit $a = a'n + r_a$ $(0 \leq r_a < n)$ et $b = b'n + r_b$ $(0 \leq r_b < n)$.

1. Si $a \equiv b \pmod{n}$ alors $r_a \equiv r_b \pmod{n}$
   et donc $r_a - r_b = kn$.
   Or $-n < r_a - r_b < n$. D'où $r_a - r_b = 0$
   et donc $r_a = r_b$.
2. Si $a = a'n + r$ et $b = b'n + r$ $(0 \leq r < n)$ alors $a - b = (a' - b')n$
   et donc $a \equiv b \pmod{n}$.

Congruence

Théorème

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors

1. $a + b \equiv a' + b' \pmod{n}$

Congrence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors

1. $a + b \equiv a' + b' \pmod{n}$
   et donc $\overline{a+b} = \overline{a' + b'}$

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\left\{\begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array}\right.$ alors

1. $a + b \equiv a' + b' \pmod{n}$
   et donc $\overline{a+b} = \overline{a' + b'}$
2. $a.b \equiv a'.b' \pmod{n}$

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors

1. $a + b \equiv a' + b' \pmod{n}$
   et donc $\overline{a+b} = \overline{a'+b'}$
2. $a.b \equiv a'.b' \pmod{n}$
   et donc $\overline{a.b} = \overline{a'.b'}$

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors

1. $a + b \equiv a' + b' \pmod{n}$
   et donc $\overline{a+b} = \overline{a'+b'}$
2. $a.b \equiv a'.b' \pmod{n}$
   et donc $\overline{a.b} = \overline{a'.b'}$
3. $a - b \equiv a' - b' \pmod{n}$

Congruence

Théorème

La congruence est compatible avec les opérations de $\mathbb{Z}$:

si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors

1. $a + b \equiv a' + b' \pmod{n}$
   et donc $\overline{a+b} = \overline{a'+b'}$
2. $a.b \equiv a'.b' \pmod{n}$
   et donc $\overline{a.b} = \overline{a'.b'}$
3. $a - b \equiv a' - b' \pmod{n}$
   et donc $\overline{a-b} = \overline{a'-b'}$

Congruence

Démonstration

Congruence

Démonstration

Si $\left\{ \begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array} \right.$ alors $\left\{ \begin{array}{c} a = a' + kn \\ b = b' + k'n \end{array} \right.$.

Congruence

Démonstration

Si $\left\{ \begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array} \right.$ alors $\left\{ \begin{array}{c} a = a' + kn \\ b = b' + k'n \end{array} \right.$.

On en déduit

Congruence

Démonstration

Si $\left\{ \begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array} \right.$ alors $\left\{ \begin{array}{l} a = a' + kn \\ b = b' + k'n \end{array} \right.$.

On en déduit

1. $a + b = a' + b' + (k + k')n$

Congruence

Démonstration

Si $\left\{ \begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array} \right.$ alors $\left\{ \begin{array}{c} a = a' + kn \\ b = b' + k'n \end{array} \right.$.

On en déduit

1. $a + b = a' + b' + (k + k')n$
   et donc $a + b \equiv a' + b' \pmod{n}$

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

Si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors $\begin{cases} a = a' + kn \\ b = b' + k'n \end{cases}$.

On en déduit

1. $a + b = a' + b' + (k + k')n$
   et donc $a + b \equiv a' + b' \pmod{n}$
2. $a.b = (a' + kn)(b' + k'n) = a'b' + (a'k' + kb' + kk'n)n$

Congruence

Démonstration

Si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors $\begin{cases} a = a' + kn \\ b = b' + k'n \end{cases}$.

On en déduit

1. $a + b = a' + b' + (k + k')n$
   et donc $a + b \equiv a' + b' \pmod{n}$
2. $a.b = (a' + kn)(b' + k'n) = a'b' + (a'k' + kb' + kk'n)n$
   et donc $a.b \equiv a'.b' \pmod{n}$

Congruence

Démonstration

Si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors $\begin{cases} a = a' + kn \\ b = b' + k'n \end{cases}$.

On en déduit

1. $a + b = a' + b' + (k + k')n$
   et donc $a + b \equiv a' + b' \pmod{n}$
2. $a.b = (a' + kn)(b' + k'n) = a'b' + (a'k' + kb' + kk'n)n$
   et donc $a.b \equiv a'.b' \pmod{n}$
3. et $a - b = a' - b' + (k - k')n$

Congruence

Démonstration

Si $\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases}$ alors $\begin{cases} a = a' + kn \\ b = b' + k'n \end{cases}$.

On en déduit

1. $a + b = a' + b' + (k + k')n$
   et donc $a + b \equiv a' + b' \pmod{n}$
2. $a.b = (a' + kn)(b' + k'n) = a'b' + (a'k' + kb' + kk'n)n$
   et donc $a.b \equiv a'.b' \pmod{n}$
3. et $a - b = a' - b' + (k - k')n$
   et donc $a - b \equiv a' - b' \pmod{n}$.

Congruence

Théorème

Congruence

Théorème

Dans $\mathbb{Z}/n\mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a}.\overline{b} = \overline{a.b}$.

Congruence

Théorème

Dans $\mathbb{Z}/n\mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a}.\overline{b} = \overline{a.b}$.
$\mathbb{Z}/n\mathbb{Z}$ muni des opérations définies ci-dessus est un anneau commutatif.

Congruence

Démonstration

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.
Remarque : $\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.
Remarque : $\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Propriété

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.
Remarque : $\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Propriété

$\forall a\ \forall b\ \overline{a}\overline{b} = \overline{ab}$.

Congruence

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\overline{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.
Remarque : $\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Propriété

$\forall a\ \forall b\ \overline{a}\,\overline{b} = a\overline{b}$.
En effet, si $a > 0$ alors $\overline{a}\,\overline{b} = \overline{ab} = \overline{b + b + \cdots + b} = a\overline{b}$.

Congruence

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

L'addition est commutative et associative, $\overline{0}$ est le neutre, $-\bar{a} = \overline{-a}$.
La multiplication est commutative et associative, $\overline{1}$ est le neutre.
La multiplication est distributive par rapport à l'addition.
Remarque : $\bar{a} - \bar{b} = \bar{a} + \overline{-b} = \overline{a + (-b)} = \overline{a - b}$.

Propriété

$\forall a \; \forall b \; \bar{a}\bar{b} = a\bar{b}$.
En effet, si $a > 0$ alors $\bar{a}\bar{b} = \overline{ab} = \overline{b + b + \cdots + b} = a\bar{b}$.
Si $a < 0$, alors $\bar{a}\bar{b} = \overline{-(-a)}\;\bar{b} = -\overline{-a}\bar{b} = -(-a)\bar{b} = a\bar{b}$.

Congruence

Eléments inversibles

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Démonstration

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Démonstration

$\overline{a}.\overline{x} = \overline{1}$ si et seulement si $\overline{ax} = \overline{1}$,

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Démonstration

$\overline{a}.\overline{x} = \overline{1}$ si et seulement si $\overline{ax} = \overline{1}$,
$ax = 1 + kn$,

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Démonstration

$\overline{a}.\overline{x} = \overline{1}$ si et seulement si $\overline{ax} = \overline{1}$,
$ax = 1 + kn$,
$ax - kn = 1$,

Congruence

Eléments inversibles

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ est inversible s'il existe $\overline{x'}$ tel que $\overline{x}.\overline{x'} = \overline{1}$.

Théorème

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, un élément $\overline{a}$ est inversible si et seulement si $PGCD(a, n) = 1$.

Démonstration

$\overline{a}.\overline{x} = \overline{1}$ si et seulement si $\overline{ax} = \overline{1}$,
$ax = 1 + kn$,
$ax - kn = 1$,
$PGCD(a, n) = 1$.

Congruence

Exemple

Congruence

Exemple

$\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$:

Congruence

Exemple

$\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$: $PGCD(3, 10) = 1$.

Congruence

Exemple

$\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$: $PGCD(3,10) = 1$.
De plus, $3.(-3) + 10.1 = 1$.

Congruence

Exemple

$\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$: $PGCD(3,10) = 1$.
De plus, $3.(-3) + 10.1 = 1$.
On en déduit $\overline{3.(-3) + 10.1} = \overline{1}$ et donc $\overline{3.(-3)} = \overline{1}$

Congruence

Exemple

$\overline{3}$ est inversible dans $\mathbb{Z}/10\mathbb{Z}$: $PGCD(3, 10) = 1$.
De plus, $3.(-3) + 10.1 = 1$.
On en déduit $\overline{3.(-3) + 10.1} = \overline{1}$ et donc $\overline{3.(-3)} = \overline{1}$
qui donne $\overline{3}.\overline{(-3)} = \overline{1}$ et $\overline{3}^{-1} = \overline{-3} = -\overline{3} = \overline{-3 + 10} = \overline{7}$.

Petit théorème de Fermat

Théorème

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod{p}$.

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod p$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod p$.

Exemple

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod{p}$.

Exemple

41 premier et $2\,007 \not\equiv 0 \pmod{41}$.

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod{p}$.

Exemple

41 premier et $2\,007 \not\equiv 0 \pmod{41}$.
On en déduit $2\,007^{41-1} \equiv 1 \pmod{41}$

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod{p}$.

Exemple

41 premier et $2\,007 \not\equiv 0 \pmod{41}$.
On en déduit $2\,007^{41-1} \equiv 1 \pmod{41}$
puis $2\,007^{40} \equiv 1 \pmod{41}$.

Petit théorème de Fermat

Théorème

Si p est premier et a n'est pas un multiple de p
alors $a^{p-1} \equiv 1 \pmod{p}$.

Corollaire

Si p est premier alors pour tout entier a, $a^p \equiv a \pmod{p}$.

Exemple

41 premier et $2\,007 \not\equiv 0 \pmod{41}$.
On en déduit $2\,007^{41-1} \equiv 1 \pmod{41}$
puis $2\,007^{40} \equiv 1 \pmod{41}$.
Le reste dans la division euclidienne de $2\,007^{40}$ par 41 est 1.

Petit théorème de Fermat

Démonstration

Petit théorème de Fermat

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$

Si $\overline{ia} = \overline{ja}$ $(1 \leq i \leq p-1,\ 1 \leq j \leq p-1)$alors $\overline{i}\,\overline{a} = \overline{j}\,\overline{a}$

Petit théorème de Fermat

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$

Si $\overline{ia} = \overline{ja}$ $(1 \leq i \leq p-1,\ 1 \leq j \leq p-1)$alors $\overline{i}\overline{a} = \overline{j}\overline{a}$

Comme a n'est pas un multiple de p, $\overline{a}$ est inversible.

Petit théorème de Fermat

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$

Si $\overline{ia} = \overline{ja}$ $(1 \leq i \leq p-1,\ 1 \leq j \leq p-1)$alors $\overline{i}\overline{a} = \overline{j}\overline{a}$

Comme a n'est pas un multiple de p, $\overline{a}$ est inversible.

On en déduit $\overline{i}\overline{a}\ \overline{a}^{-1} = \overline{j}\overline{a}\ \overline{a}^{-1}$

puis $\overline{i} = \overline{j}$, $i = j + kp$ et $i - j = kp$.

Petit théorème de Fermat

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$
Si $\overline{ia} = \overline{ja}$ $(1 \leq i \leq p-1,\ 1 \leq j \leq p-1)$alors $\overline{i}\overline{a} = \overline{j}\overline{a}$
Comme a n'est pas un multiple de p, $\overline{a}$ est inversible.
On en déduit $\overline{i}\overline{a}\ \overline{a}^{-1} = \overline{j}\overline{a}\ \overline{a}^{-1}$
puis $\overline{i} = \overline{j}$, $i = j + kp$ et $i - j = kp$.
Par ailleurs $1 \leq i \leq p-1$, $1 \leq j \leq p-1$ donne
$1-(p-1) \leq i-j \leq p-1-1$ soit $-(p-2) \leq i-j \leq p-2$.

Petit théorème de Fermat

Démonstration

On montre d'abord $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \{\overline{0}, \overline{a}, \overline{2a}, \cdots, \overline{(p-1)a}\}$
Si $\overline{ia} = \overline{ja}$ $(1 \leq i \leq p-1,\ 1 \leq j \leq p-1)$alors $\overline{i}\overline{a} = \overline{j}\overline{a}$
Comme a n'est pas un multiple de p, $\overline{a}$ est inversible.
On en déduit $\overline{i}\overline{a}\ \overline{a}^{-1} = \overline{j}\overline{a}\ \overline{a}^{-1}$
puis $\overline{i} = \overline{j}$, $i = j + kp$ et $i - j = kp$.
Par ailleurs $1 \leq i \leq p-1$, $1 \leq j \leq p-1$ donne
$1-(p-1) \leq i-j \leq p-1-1$ soit $-(p-2) \leq i-j \leq p-2$.
On a donc $i - j = 0.p = 0$ et $i = j$.

Petit théorème de Fermat

Démonstration

Démonstration

On en déduit $\overline{a}\,\overline{2a}\,\overline{3a}\cdots\overline{(p-1)a} = \overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Démonstration

On en déduit $\overline{a}\,\overline{2a}\,\overline{3a}\cdots\overline{(p-1)a} = \overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.
puis $\overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}\,\overline{a}^{p-1} = \overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.

Petit théorème de Fermat

Démonstration

On en déduit $\overline{a}\,\overline{2a}\,\overline{3a}\cdots\overline{(p-1)a} = \overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.
puis $\overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}\,\overline{a}^{p-1} = \overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.
Comme tous les $\overline{i}$ $(1 \leq i \leq p-1)$ sont inversibles, on a

Petit théorème de Fermat

Démonstration

On en déduit $\overline{a}\,\overline{2a}\,\overline{3a}\cdots\overline{(p-1)a}=\overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.
puis $\overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}\,\overline{a}^{p-1}=\overline{1}\,\overline{2}\,\overline{3}\cdots\overline{(p-1)}$.
Comme tous les $\overline{i}$ $(1\leq i\leq p-1)$ sont inversibles, on a $\overline{a}^{p-1}=\overline{1}$, $\overline{a^{p-1}}=\overline{1}$ et $a^{p-1}\equiv 1 \pmod{p}$

Petit théorème de Fermat

Démonstration du corollaire

Petit théorème de Fermat

Démonstration du corollaire

Si a n'est pas un multiple de p,

Petit théorème de Fermat

Démonstration du corollaire

Si a n'est pas un multiple de p, $\overline{a}^{p-1} = \overline{1}$ entraîne $\overline{a}^{p-1}\,\overline{a} = \overline{1}\,\overline{a}$

Petit théorème de Fermat

Démonstration du corollaire

Si a n'est pas un multiple de p, $\overline{a}^{p-1} = \overline{1}$ entraîne $\overline{a}^{p-1}\,\overline{a} = \overline{1}\,\overline{a}$ et donc $\overline{a}^{p} = \overline{a}$.

Petit théorème de Fermat

R3.09 Cryptographie et sécurité

Département Informatique

Démonstration du corollaire

Si a n'est pas un multiple de p, $\overline{a}^{p-1} = \overline{1}$ entraîne $\overline{a}^{p-1}\,\overline{a} = \overline{1}\,\overline{a}$ et donc $\overline{a}^p = \overline{a}$.
Si a est un multiple de p, $\overline{a}^p = \overline{a} = \overline{0}$.

Théorème du reste chinois

Théorème

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux ($m \geq 2$, $n \geq 2$)

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux $(m \geq 2,\ n \geq 2)$
alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux ($m \geq 2$, $n \geq 2$)
alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ a pour solution $S = \{x_0 + kmn, \ k \in \mathbb{Z}\}$ avec x_0 solution particulière du système.

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux ($m \geq 2$, $n \geq 2$)
alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ a pour solution $S = \{x_0 + kmn,\ k \in \mathbb{Z}\}$ avec x_0 solution particulière du système.

Remarques

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux $(m \geq 2,\ n \geq 2)$
alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ a pour solution $S = \{x_0 + kmn,\ k \in \mathbb{Z}\}$ avec x_0 solution particulière du système.

Remarques

1. $S = \{x_0 + kmn,\ k \in \mathbb{Z}\} = \{x \in \mathbb{Z},\ x \equiv x_0 \pmod{mn}\}$

Théorème du reste chinois

Théorème

Soient a et b deux entiers quelconques.
Si m et n sont premiers entre eux ($m \geq 2$, $n \geq 2$)
alors $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ a pour solution $S = \{x_0 + kmn,\ k \in \mathbb{Z}\}$ avec x_0 solution particulière du système.

Remarques

1. $S = \{x_0 + kmn,\ k \in \mathbb{Z}\} = \{x \in \mathbb{Z},\ x \equiv x_0 \pmod{mn}\}$
2. En notant $mu + nv = 1$ (décomposition de Bezout), on peut prendre $x_0 = mub + nva$.

Théorème du reste chinois

Démonstration

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\left\{\begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array}\right.$

On a $\left\{\begin{array}{l} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{array}\right.$

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m|x - x_0$ et $n|x - x_0$ avec $PGCD(m, n) = 1$.

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m|x - x_0$ et $n|x - x_0$ avec $PGCD(m, n) = 1$.

On a donc $mn|x - x_0$

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m|x - x_0$ et $n|x - x_0$ avec $PGCD(m, n) = 1$.

On a donc $mn|x - x_0$ et $x - x_0 = kmn$ $(k \in \mathbb{Z})$.

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m | x - x_0$ et $n | x - x_0$ avec $PGCD(m, n) = 1$.

On a donc $mn | x - x_0$ et $x - x_0 = kmn$ $(k \in \mathbb{Z})$.

Réciproquement, $x_0 + kmn \equiv a \pmod{m}$

Théorème du reste chinois

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m|x - x_0$ et $n|x - x_0$ avec $PGCD(m, n) = 1$.
On a donc $mn|x - x_0$ et $x - x_0 = kmn$ ($k \in \mathbb{Z}$).
Réciproquement, $x_0 + kmn \equiv a \pmod{m}$
et $x_0 + kmn \equiv b \pmod{n}$.

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Démonstration

Soit x_0 une solution particulière de $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

On a $\begin{cases} x_0 \equiv a \pmod{m} \\ x_0 \equiv b \pmod{n} \end{cases}$

On en déduit $\begin{cases} x - x_0 \equiv 0 \pmod{m} \\ x - x_0 \equiv 0 \pmod{n} \end{cases}$

et donc $m|x - x_0$ et $n|x - x_0$ avec $PGCD(m, n) = 1$.

On a donc $mn|x - x_0$ et $x - x_0 = kmn$ $(k \in \mathbb{Z})$.

Réciproquement, $x_0 + kmn \equiv a \pmod{m}$

et $x_0 + kmn \equiv b \pmod{n}$.

$S = \{x_0 + kmn,\ k \in \mathbb{Z}\}$.

Théorème du reste chinois

Démonstration

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Démonstration

Comme $PGCD(m,n) = 1$, $\exists u,\ v\ mu + nv = 1$.

Théorème du reste chinois

Démonstration

Comme $PGCD(m, n) = 1$, $\exists u,\ v\ mu + nv = 1$.
$mub + nva = mub + (1 - mu)a = a + (b - a)um \equiv a \pmod{m}$.

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Démonstration

Comme $PGCD(m, n) = 1$, $\exists u,\ v\ mu + nv = 1$.
$mub + nva = mub + (1 - mu)a = a + (b - a)um \equiv a \pmod{m}$.
$mub + nva = (1 - nv)b + nva = b + (a - b)vn \equiv b \pmod{n}$.

Théorème du reste chinois

Démonstration

Comme $PGCD(m,n) = 1$, $\exists u,\ v\ mu + nv = 1$.
$mub + nva = mub + (1 - mu)a = a + (b - a)um \equiv a \pmod{m}$.
$mub + nva = (1 - nv)b + nva = b + (a - b)vn \equiv b \pmod{n}$.
On en déduit que $x_0 = mub + nva$ est une solution particulière de
$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}.$$

Théorème du reste chinois

Exemple

Théorème du reste chinois

Exemple

Mon panier peut contenir au plus cent oeufs.
Si je le vide par trois oeufs à la fois, il en reste un, si je le vide par huit oeufs à la fois, il en reste deux, et si je le vide par sept oeufs à la fois, il en reste cinq.
Combien ai-je d'oeufs?
Manuscrit chinois de Sun-Tsu (1^{er} siècle).

Théorème du reste chinois

Exemple

Mon panier peut contenir au plus cent oeufs.
Si je le vide par trois oeufs à la fois, il en reste un, si je le vide par huit oeufs à la fois, il en reste deux, et si je le vide par sept oeufs à la fois, il en reste cinq.
Combien ai-je d'oeufs?
Manuscrit chinois de Sun-Tsu (1er siècle).
Mise en équation

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Exemple

Mon panier peut contenir au plus cent oeufs.
Si je le vide par trois oeufs à la fois, il en reste un, si je le vide par huit oeufs à la fois, il en reste deux, et si je le vide par sept oeufs à la fois, il en reste cinq.
Combien ai-je d'oeufs?
Manuscrit chinois de Sun-Tsu (1^{er} siècle).
Mise en équation

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \\ 0 \leq x \leq 100 \end{cases}$$

Théorème du reste chinois

Exemple

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{8} \\ x \equiv 5 \pmod{7} \end{cases}$$

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases}$$

$3.3 + 8.(-1) = 1$ donne $x_0 = 3.3.2 + 8.(-1).1 = 10$

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases}$$

$3.3 + 8.(-1) = 1$ donne $x_0 = 3.3.2 + 8.(-1).1 = 10$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \end{cases} \Leftrightarrow x \equiv 10 \pmod{24}$$

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases}$$

$3.3 + 8.(-1) = 1$ donne $x_0 = 3.3.2 + 8.(-1).1 = 10$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \end{cases} \Leftrightarrow x \equiv 10 \pmod{24}$$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv 10 \pmod{24} \\ x \equiv 5 \pmod 7 \end{cases}$$

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases}$$

$3.3 + 8.(-1) = 1$ donne $x_0 = 3.3.2 + 8.(-1).1 = 10$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \end{cases} \Leftrightarrow x \equiv 10 \pmod{24}$$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases} \Leftrightarrow \begin{cases} x \equiv 10 \pmod{24} \\ x \equiv 5 \pmod 7 \end{cases}$$

$24.(-2) + 7.7 = 1$ donne $x_0' = 24.(-2).5 + 7.7.10 = -240 + 490 = 250$

Théorème du reste chinois

Exemple

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{8} \\ x \equiv 5 \pmod{7} \end{cases} \Leftrightarrow x \equiv 250 \pmod{24.7} \Leftrightarrow x \equiv 250 \pmod{168}$$

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases} \Leftrightarrow x \equiv 250 \pmod{24.7} \Leftrightarrow x \equiv 250 \pmod{168}$$

Or $250 = 168.1 + 82$.

Donc $x \equiv 250 \pmod{168} \Leftrightarrow x \equiv 82 \pmod{168}$

Théorème du reste chinois

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois

Exemple

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \end{cases} \Leftrightarrow x \equiv 250 \pmod{24.7} \Leftrightarrow x \equiv 250 \pmod{168}$$

Or $250 = 168.1 + 82$.

Donc $x \equiv 250 \pmod{168} \Leftrightarrow x \equiv 82 \pmod{168}$

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 8 \\ x \equiv 5 \pmod 7 \\ 0 \leq x \leq 100 \end{cases} \Leftrightarrow x = 82$$

R3.09 Cryptographie et sécurité

Département Informatique

Plan

Congruence

Petit théorème de Fermat

Théorème du reste chinois