

Leçon 45 - Nombres premiers

Leçon 45 - Nombres premiers

- Nombres premiers

- Valuations

- 4 Deablance
- 2. Théorème d'Euclide
- 2.1. Définit
- 2.2. Lemmes d'Euclide
- 2.3. Theoreme tondamenta
 - ombres premier
 - 3.2. Crible d'Eratosth
- 4. Valuation
- p-adique)
- 4.1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- premiers
- 4.4. Formule de Legend
- 5 Petit Fermat
 - 5.1. Motivation
 - i.2. Enoncé et app

- ⇒ Nombres premiers
- \Rightarrow Valuations p-adique
- ⇒ Petit théorème de Fermat.
- 1. Problèmes
- 2. Théorèmes d'Euclide
 - 2.1. Définition
 - 2.2. Lemmes d'Euclide
 - 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - 3.1. Ensemble infini
 - 3.2. Crible d'Eratosthène
- 4. Valuation (p-adique)
 - 4.1. Fonction valuation (en base p)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
- 5. Garantir que des nombres sont premiers
 - 5.1. Motivations

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

5.2. Enoncé et applications

5.3. Démonstrations

Leçon 45 - Nombres premiers

⇒ Nombres p

- Botit Format

1. Problèmes

- Théorèmes d'Euclide
- 2.1 Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- L'ensemble des nombres premiers
 - 3.1. Ensemble infini
 - 3.2. Crible d'Eratosthèn
 - . Valuation
 - 4.1. Fonction valuation
 - 4.0. Manabiana (da manatida
- 4.3 Factorisation on produit
 - 4 Formula de Lagando
 - D-10 F-----
- 5.1. Motivation
- 5.2. Enoncé et
 - 3. Démonstrations

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1. Problèmes

4 Valuation

Problèmes

Problème - Produit de premiers

Leçon 45 - Nombres premiers

⇒ Nombres p

> valuation -adique

⇒ Petit Fermat

1. Problèmes

- Théorèmes d'Euclide
 - Lucilde
 - .2. Lemmes d'Euclide
 - 2.3. Théorème fondamenta
- L'ensemble des nombres premiers
 - .1. Ensemble infini
 - .2. Crible d'Eratosthèr
 - Valuation valuation
- I.1. Fonction valuation
- 2 Morobiema (da monoida)
- 4.2. Morphisme (de monoide)
- premiers
- 1.4. Formule de Legend
- 5. Petit Fermat
- 5.1. Motivation
- ---
 - 3. Démonstrations

Problèmes

Problème - Produit de premiers

Problème - Constructions de cours

Leçon 45 - Nombres premiers

→ Nombres p

-adique

⇒ Petit Fermat

1. Problèmes

- Théorèmes d'Euclide
 - Euclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - Ensemble infini
 - 3.2. Crible d'Eratosthène
 - Valuation -adique)
 - 1 Fonction valuati
 - 2 Marchisma (do manaida)
- 4.2. Morphisme (de monoïde)
- premiers
 - I. Formule de Legendre

5. Petit Fermat

- 5.1. Motivation
- 5.2. Enoncé et
 - . Démonstrations

Problèmes

Problème - Produit de premiers

Problème - Constructions de cours

Problème - Fonctions arithmétiques

Lecon 45 - Nombres premiers

1. Problèmes

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 2.1. Définition
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

2.1 Définition

4 Valuation

Notion absolue

Il ne s'agit plus d'une notion relative comme précédemment (a et b sont premiers entre eux). Ici, il s'agit d'une notion absolue.

Leçon 45 - Nombres premiers

→ Nombres p

p-adique

⇒ Petit Fermat

- 1. Problèmes
 - . Théorèmes 'Euclide
- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 3. L'ensemble des nombres premiers
 - 1. Ensemble infini
- 3.2. Crible d'Eratosthè
- Valuation
- I 1 Econtico univerti
- 1.2 Morphisma (da monolida)
- 4.2. Morphisme (de monoide)
 - Formule de Legendr
 - .4. Formule de Legendre
- b. Petit Fermat
- 5.1. Motivations
- .z. Enonce et ap

Notion absolue

Il ne s'agit plus d'une notion relative comme précédemment (a et b sont premiers entre eux). Ici, il s'agit d'une notion absolue.

Définition - Nombre premier

Soit $p \in \mathbb{N}^*$.

On dit que p est (un nombre) premier

si $p \neq 1$ et si les seuls diviseurs de p dans \mathbb{N} sont 1 et p.

On note souvent \mathcal{P} , l'ensemble des nombres premiers.

Leçon 45 - Nombres premiers

⇒ Valuation

⇒ Petit Ferma

Problèmes

. Théorèmes l'Euclide

- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
- 3.2. Crible d'Eratosthèn
- J.Z. CHOIC G ETAIUSTITE
- . Valuation p-adique)
- .1. Fonction valuation
- .1. Fonction valuation
- .2. Morphisme (de monoide)
- premiers
- 4. Formule de Legendr

5. Petit Fermat

- 1. Motivations
- i.2. Enoncé et ap

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide

 - 2.2. Lemmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base p)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

2.2 Lammas d'Euclida

4 Valuation

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Leçon 45 - Nombres premiers

→ Nombres _I

⇒ Valuation
-adique

⇒ Petit Ferma

1. Problèmes

2. Théorèmes l'Euclide

1. Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

1. Ensemble infir

3.2. Crible d'Eratosthèr

Valuation -adique)

- 4.1. Fonction valua
- 4.2 Morphisma (do manaida)
- 4.3. Factorisation en produit d
 - 4. Formule de Legendr

4.4. Formule de Legendi

E 1 Mativation

5.1. IVIULIVALIUI

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Proposition - Premier théorème d'Euclide

Un nombre premier est premier avec tous les entiers qu'il ne divise pas.

Un nombre premier divise un produit si et seulement si il divise l'un des facteurs.

Leçon 45 - Nombres premiers

→ Valuations

⇒ Petit Ferma

- 1. Problèmes
- Théorème: d'Euclide
- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 3. L'ensemble des
 - mbres premier
 - .2. Crible d'Eratosthèn
- Crible d'Eratosthe
 Valuation
 - p-adique)
 - .1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- oremiers
- 4. Formule de Legendr
- 5. Petit Fermat
- 5.1. Motivation:
- 5.2. Enoncé et app

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Proposition - Premier théorème d'Euclide

Un nombre premier est premier avec tous les entiers qu'il ne divise pas.

Un nombre premier divise un produit si et seulement si il divise l'un des facteurs.

Démonstration

Leçon 45 - Nombres premiers

→ Valuation

⇒ Petit Ferma

- 1. Problèmes
- 2. Théorèmes d'Euclide
- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 3. L'ensemble des nombres premiers
 - Ensemble infini
- 3.2. Crible d'Eratosthèn
- 4 Valuation
 - Fonction valuation
 - .1. Fonction valuation
- 4.2. Morphisme (de monoîde)
- oremiers
- 4. Formule de Legendr

5. Petit Fermat

- 5.1. Motivation
- 2. Enoncé et app

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Proposition - Premier théorème d'Euclide

Un nombre premier est premier avec tous les entiers qu'il ne divise pas.

Un nombre premier divise un produit si et seulement si il divise l'un des facteurs.

Démonstration

L'intérêt des nombres premiers est d'être une brique élémentaire multiplicative de \mathbb{Z} , on ne peut la couper en deux.

Savoir-faire. Trouver un facteur, avec un nombre premier

Soit $p \in \mathcal{P}$ tel que p|ab alors p|a ou p|b.

Ce n'est pas le cas de p = 12 qui divise 6×4 avec a = 6 et b = 4.

- 1 Problèmes
- 2.2. Lemmes d'Euclide

- 4 Valuation

Théorème -

Tout entier naturel $n \ge 2$ possède au moins un diviseur premier.

Leçon 45 - Nombres premiers

⇒ Nombres p

→ Petit Ferma

. Problèmes

. Théorèmes 'Euclide

2.1. Définition

2.2. Lemmes d'Euclide

L'ensemble des nombres premiers

Ensemble infini

3.2. Crible d'Eratosthèr

. Valuation p-adique)

- 4.1. Fonction valuation
- 4.2 Morphisms (do monsido)
- 4.2. Morphisme (de monoide)
- premiers
 - Formule de Legendre

5. Petit Fermat

- 5.1. Motivations
- 5.2. Enoncé et a
 - Démonstrations

Théorème -

Tout entier naturel $n \ge 2$ possède au moins un diviseur premier.

Démonstration

Lecon 45 - Nombres premiers

- 2.2. Lemmes d'Euclide

Théorème -

Tout entier naturel $n \ge 2$ possède au moins un diviseur premier.

Démonstration

Corollaire - Critère de primalité entre deux entiers

Soient $a, b \in \mathbb{Z}$.

Alors a et b sont premiers entre eux si et seulement s'ils n'ont aucun diviseur premier en commun.

Lecon 45 - Nombres premiers

1 Problèmes

2.2. Lemmes d'Euclide

Théorème -

Tout entier naturel $n \ge 2$ possède au moins un diviseur premier.

Démonstration

Corollaire - Critère de primalité entre deux entiers

Soient $a, b \in \mathbb{Z}$.

Alors a et b sont premiers entre eux si et seulement s'ils n'ont aucun diviseur premier en commun.

Démonstration

Lecon 45 - Nombres premiers

1 Problèmes

2.2. Lemmes d'Euclide

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide

 - 2.3. Théorème fondamental
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

2.3. Théorème fondamental

4 Valuation

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Leçon 45 - Nombres premiers

→ Valuations

⇒ Petit Fermat

- 1. Problèmes
- 2. Théorèmes d'Euclide
- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- L'ensemble des nombres premiers
 - .1. Ensemble infini
- 3.2. Crible d'Eratosthè
- I. Valuation p-adique)
- 4.1. Fonction valuation
- 4.2 Morohisme (de monoïde
- 4.2. Morphisme (de monoide)
- premiers
- 4.4. Formule de Legen
- 5. Petit Ferma
- 5.1. Motivation
- 5.2. Enonce et:

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers

Soit $n \in \mathbb{N}$, $n \ge 2$.

Alors il existe $r \in \mathbb{N}$, $p_1, \dots p_r$, r nombres premiers (distincts) et $\alpha_1, \alpha_2, \dots \alpha_r \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^r p_i^{\alpha_i}$$

Cette écriture est unique.

Leçon 45 - Nombres premiers

→ Valuation
-adique

⇒ Petit Ferma

- 1. Problèmes
- Théorèmes
 Euclide
- .1. Definition
- 2.3. Théorème fondamental
- 3. L'ensemble des
- nombres premiers
- 3.2. Crible d'Eratosthène
- 3.2. Crible d'Eratosthèr
- 4. Valuation (p-adique)
 - 1.1. Fonction valuation
 - 2 Morphisma (da monolida)
 - 1.2. Morphisme (de monoïde)
 - remiers
- 4.4. Formule de Legendi

5. Petit Fermat

- .1. Motivations
- 5.2. Enonce et a
 - Démonstrations

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers

Soit $n \in \mathbb{N}$, $n \ge 2$.

Alors il existe $r \in \mathbb{N}$, $p_1, \dots p_r$, r nombres premiers (distincts) et $\alpha_1, \alpha_2, \dots \alpha_r \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^r p_i^{\alpha_i}$$

Cette écriture est unique.

Démonstration

Lecon 45 - Nombres

- 1. Problèmes

- 2.3. Théorème fondamental

- 4 Valuation

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 3.1. Ensemble infini
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

3.1 Ensemble infini

4 Valuation

Théorème d'Euclide

Proposition - (Second) théorème d'Euclide

L'ensemble des nombres premiers, noté \mathscr{P} (parfois \mathbb{P}) est infini.

Lecon 45 - Nombres premiers

- 1. Problèmes

- 3.1. Ensemble infini

Théorème d'Euclide

Proposition - (Second) théorème d'Euclide

L'ensemble des nombres premiers, noté ${\mathscr P}$ (parfois ${\mathbb P}$) est infini.

Démonstration

Leçon 45 - Nombres premiers

Nombres pr

. . . .

1. Problèmes

Théorèmes d'Euclide

2.1. Définition

2.3. Théorème fondamenta

3. L'ensemble des nombres premiers

nombres premiers
3.1. Ensemble infini

.2. Crible d'Eratosthé

Valuation

p-adique)

1. Fonction valuation

.2. Morphisme (de monoïde)

4.2. Morphisme (de monoīde)

remiers

I. Formule de Legendre

Petit Ferma

5.1. Motivations

5.2. Enoncé et a

Démonstrations

Description énumérative de 🎐

Remarque Ensemble dénombrable

Leçon 45 - Nombres premiers

→ Nullibres p

1. Problèmes

2. Théorèmes

- d'Euclide
- 2.1. Définition
- 2.2. Denimes a Laurae
- L'ensemble des nombres premiers
- 3.1. Ensemble infini
- 3.2. Crible d'Eratosthi
 - Valuation
- 4.1 Fonction valuation
- 4.0 Managina (da manafida)
- 4.2. Morphisme (de monoïde)
- premiers
- 4.4. Formule de Legen

Petit Ferma

- 5.1. Motivation
- 5.2. Enoncé e
 - . Démonstrations

Description énumérative de ${\mathscr P}$

Remarque Ensemble dénombrable

Proposition - Enumération des nombres premiers

Il existe une bijection $p: \mathbb{N}^* \to \mathcal{P}, i \mapsto p_i$, le i-ième nombre premier.

Leçon 45 - Nombres premiers

y redinibles p

- Potit Format

1. Problèmes

Théorèmes d'Euclide

2.1 Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

3.1. Ensemble infini

Crible d'Eratosthère

Valuation

p-adique)

I.1. Fonction valuation

4.2. Morphisme (de monoïde)

oremiers

4. Formule de Legendr

5. Petit Ferma

5.1. Motivations

Enoncé et app

Description énumérative de ${\mathscr P}$

Remarque Ensemble dénombrable

Proposition - Enumération des nombres premiers

Il existe une bijection $p: \mathbb{N}^* \to \mathscr{P}, i \mapsto p_i$, le i-ième nombre premier.

Exercice Que vaut p_{10} ?

Leçon 45 - Nombres premiers

> Valuations

⇒ Petit Fermat

1. Problèmes

Théorèmes d'Euclide

2.1. Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

nombres premiers 3.1. Ensemble infini

2. Crible d'Eratosthè

Valuation

p-adique)

1. Fonction valuation

Morphisme (de monoïde)

4.2. Morphisme (de monoīde)

premiers

4. Formule de Legendr

5. Petit Fermat

5.1. Motivations

2. Enoncé et app

Description énumérative de ${\mathscr P}$

Remarque Ensemble dénombrable

Proposition - Enumération des nombres premiers

Il existe une bijection $p: \mathbb{N}^* \to \mathscr{P}, i \mapsto p_i$, le i-ième nombre premier.

Exercice Que vaut p_{10} ?

Démonstration

Leçon 45 - Nombres premiers

> Valuations

⇒ Petit Fermat

1. Problèmes

Théorèmes d'Euclide

2.1. Définition

2.2. Lemmes d Euclide

3. L'ensemble des

nombres premiers
3.1. Ensemble infini

2. Crible d'Eratosthè

Valuation

. valuation p-adique)

.1. Fonction valuation

.2. Morphisme (de monoide)

4.2. Morphisme (de monoide)
4.3. Factorisation en produit de

oremiers

.4. Formule de Legendr

Petit Fermat

5.1. Motivations

2. Enoncé et app

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers

 - 3.2. Crible d'Eratosthène
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

3.2 Crible d'Erstoethène 4 Valuation

Crible d'Eratosthène

Pour obtenir la liste des nombres premiers, nous n'avons pas trouvé beaucoup mieux que le crible d'Eratosthène (3-ième siècle avant J-C).

Il s'agit d'écrire la liste des entiers de 1 à n. Puis d'enlever les multiples des nombres qui restent. Une fois terminée (deux boucles), il ne reste que la liste des nombres premiers plus petit que n.

Leçon 45 - Nombres premiers

→ Valuation
-adique

⇒ Petit Ferma

1. Problèmes

2. Théorèmes d'Euclide

2.1. Défin

2.2. Lemmes d'Euclide

3. L'ensemble des nombres premiers

3.1. Ensemble infini
 3.2. Crible d'Eratosthène

3.2. Crible d Eratostne

4. Valuation (p-adique)

1. Fonction valuatio

- I.2. Morphisme (de monoide)
- oremiers
- 4.4. Formule de Legend

5. Petit Fermat

5.1. Motivation

- 2. Enoncé et ap
- . Démonstrations

Leçon 45 - Nombres premiers

Python - Crible d'Eratosthène

```
def Eratosthene(n):
        """ Crible d'Erathostene adapte """
2
        L = [1] * n
3
        for k in range(2,n):
             if L[k]==1 :
                 h=2*k
                 while h<n :
                     L[h]=0
                     h=h+k
        P = []
10
        for k in range(1,n):
11
             if L[k]==1:
12
                 P=P+[k]
13
        return(P)
14
```

Voluetiene

⇒ Petit Fermat

1. Problèmes

. Théorèmes l'Euclide

2.1. Définit

2.2. Lemmes d'Euclide

3. L'ensemble des nombres premiers

nombres premiers
3.1. Ensemble infini

3.2. Crible d'Eratosthène

4. Valuation (p-adique)

4.1. Fonction valuatio

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de

4.4. Formule de Legendr

....

5.1. Motivations

5.2 Enoncé et a

Culture

Remarque Conjectures

Leçon 45 - Nombres premiers

> Nombres premie

⇒ Valuation
-adique

⇒ Petit Ferma

. Problèmes

. Théorèmes 'Euclide

- Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamenta
- 3. Lensemble des nombres premiers
- 3.2. Crible d'Eratosthène
- 3.2. Crible d'Eratosthène

Valuation

- .1. Fonction valuat
- 2 Morohisme (de monoide)
- 4.2. Morprisme (de monoide)
- premiers
- .4. Formule de Legendr

5.1. Motivation

- J. 1. 1910 (1944) 011.
- E 2 Dámonetration

Culture

Remarque Conjectures

Un résultat culturel (mais pas nécessairement à retenir)

Théorème de Hadamard - De la Vallée Poussin (1896)

Notons $\pi(n)$, le nombre de nombres premiers plus petit que n. Alors

$$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln n}$$

Leçon 45 - Nombres premiers

→ Valuation
adique

⇒ Petit Ferma

- 1. Problèmes
- 2. Théorèmes d'Euclide
- 2.1. Définitio
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
- 3.2. Crible d'Eratosthène
- Valuation
- . Valuation
- 1. Fonction valuation
- .2. Morohisme (de monoïde)
- remiers
- 4. Formule de Legendre
- 5. Petit Fermat
- 5.1. Motivations
- .2. Enonce et appi

Remarque Conjectures

Un résultat culturel (mais pas nécessairement à retenir)

Théorème de Hadamard - De la Vallée Poussin (1896)

Notons $\pi(n)$, le nombre de nombres premiers plus petit que n. Alors

$$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln n}$$

Le livre Merveilleux nombres premiers de Jean-Paul Delahaye donne une foule d'informations et d'anecdotes concernant les nombres premiers (par exemple : l'histoire des jumeaux John et Michael qui voient les nombres premiers...).

Lecon 45 - Nombres premiers

- 1 Problèmes
- 2 Théorèmes

- 3.2 Crible d'Eratosthène
- 4 Valuation

Evaluation de p_{1000}

Exercice

En exploitant le théorème de Hadamard-De la Vallée Poussin, donner une valeur approchée de p_{1000}

Leçon 45 - Nombres premiers

→ Valuations

→ Petit Fermat

1. Problèmes

Théorèmes d'Euclide

- 2.1 Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamenta
- 3. L'ensemble des nombres premiers
 - Ensemble infini
- 3.2. Crible d'Eratosthène

Valuation

- . , L1 Fonction valuation
- 2. Marahisma (da manaida)
- 4.2. Morphisme (de monoide)
 - 4. Formule de Legendre

4.4. Formule de Legendre

5.1. Motivations

- 5.1. Motivation
- .2. Enonce et appi

- ⇒ Nombres premiers \Rightarrow Valuations p-adique
 - ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base p)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

4.1. Fonction valuation

Définition

Définition - Valuation p-adique

Soit p un nombre premier. Pour $n \in \mathbb{N}$, on appelle *valuation* p-adique de n le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n. On le note $v_p(n)$.

Leçon 45 - Nombres premiers

→ Valuation→ adique

⇒ Petit Ferma

- Problèmes
- Théorème d'Euclide
- 2.1. Définition
- 2.2. Letitilles à Lucilde
 2.3. Théorème fondamental
- 3. L'ensemble des
- Ensemble infini
- 3.2. Crible d'Eratosthè
- Valuation
- 4.1. Fonction valuation
- 4.2 Marahiama (da manaida)
- 4.2. Morphisme (de monoide)
- 1.4. Formule de Legend
- 5. Petit Fermat
 - 5.1. Motivations
 - 5.2. Enonce et:

2. Théorèmes d'Euclide

2.1. Définition

2.2. Lettimes d'Euclide
2.3 Théorème fondemental

3. L'ensemble des

nombres premiers

3.2. Crible d'Eratosthène

3.2. Crible d Eratostne

4. Valuation (p-adique)

4.1. Fonction valuation

4.2. Morphisme (de monoïde)

I.3. Factorisation en produit de

l.4. Formule de Legend

_ . _

5. Pelil Ferria

1. Motivations

.z. Enonce et appi

Définition - Valuation p-adique

Soit p un nombre premier. Pour $n \in \mathbb{N}$, on appelle *valuation* p-adique de n le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n. On le note $v_p(n)$.

On a les caractérisations suivantes, qu'il faut savoir exploiter comme savoir-faire :

Savoir-faire. Caractérisation

$$p^{k}|a \Longleftrightarrow v_{p}(a) \geqslant k$$

$$(a = p^{h}q \text{ et } p \land q = 1) \Longleftrightarrow v_{p}(a) = h$$

.1. Definition

2.2. Denimes a coolide

3. L'ensemble des

nombres premiers

3.2. Crible d'Eratosth

J.Z. Office d Liaios

. Valuation p-adique)

4.1. Fonction valuation

4.2. Morphisme (de monoïde)

Morphisme (de monoide)
 Factorisation en produit de

.4. Formule de Legend

4.4. I Officiale de Legan

5. Petit Fermat

5.1. Motivation

5.2. Enonce et app

Définition - Valuation p-adique

Soit p un nombre premier. Pour $n \in \mathbb{N}$, on appelle *valuation* p-adique de n le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n. On le note $v_p(n)$.

On a les caractérisations suivantes, qu'il faut savoir exploiter comme savoir-faire :

Savoir-faire. Caractérisation

$$p^{k}|a \Longleftrightarrow v_{p}(a) \geqslant k$$

$$(a = p^{h}q \text{ et } p \land q = 1) \Longleftrightarrow v_{p}(a) = h$$

Démonstration

Réécriture

Exercice

Montrer que $v_p(pb) = 1 + v_p(b)$

Lecon 45 - Nombres premiers

1. Problèmes

- 4.1. Fonction valuation

Réécriture

Exercice

Montrer que $v_p(pb) = 1 + v_p(b)$

Remarque Réécriture du théorème fondamental de l'arithmétique

Lecon 45 - Nombres premiers

- 1. Problèmes

- 4.1. Fonction valuation

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

4.2. Morphisme (de monoïde)

Propriété logarithmique

Proposition - Valuation, fonction logarithmique

Pour tout $a, b \in \mathbb{Z}$ et $p \in \mathcal{P}$, $v_p(a \times b) = v_p(a) + v_p(b)$

Leçon 45 - Nombres premiers

→ Nombres p

o usiquo

Problèmes

I héorémes d'Euclide

2.1 Définition

2.2. Lemmes d'Euclide

3 L'ancomble dec

. Ensemble infini

Crible d'Eratosthèr

3.2. Crible d'Eratosthène

J-adique)

Fonction valuation

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit

. Formule de Legendre

5. Petit Fermat

5.1. Motivations

5.2. Enonce et:

. Démonstrations

Propriété logarithmique

Proposition - Valuation, fonction logarithmique

Pour tout $a, b \in \mathbb{Z}$ et $p \in \mathcal{P}$, $v_p(a \times b) = v_p(a) + v_p(b)$

Démonstration

Lecon 45 - Nombres premiers

- 1. Problèmes

- 4.2. Morphisme (de monoïde)

- ⇒ Nombres premiers \Rightarrow Valuations p-adique
 - ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base p)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

4.3 Factorisation en produit de

Factorisations, *PGCD* et *PPCM*

Proposition - Liste des diviseurs

Soient $a,b\in\mathbb{N}$ non nuls. Si $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ et $b=p_1^{\beta_1}\dots p_k^{\beta_k}$ où les p_i sont des premiers distincts 2 à 2, $\alpha_i,\beta_i\in\mathbb{N}$, alors $a|b\Longleftrightarrow \forall i\in \llbracket 1,k \rrbracket, \alpha_i\leqslant \beta_i$ $a\land b=\prod_{i=1}^k p_i^{\min(\alpha_i,\beta_i)}$ et $a\lor b=\prod_{i=1}^k p_i^{\max(\alpha_i,\beta_i)}$

Leçon 45 - Nombres premiers

→ Valuations

→ Petit Ferma

- 1. Problèmes
- Théorèmes d'Euclide
- 2.1. Definition
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - 1. Ensemble infini
 - 3.2. Crible d'Eratosthè
- 4. Valuation
- 1.1. Fonction valuation
- .1. Fonction valuation

 2. Morphisme (de monoide)
- 4.3. Factorisation en produit de
 - 4. Formule de Legend
- 5. Petit Fermat
 - 5.1. Motivations
 - .2. Enoncé et appl

Proposition - Liste des diviseurs

Soient $a,b\in\mathbb{N}$ non nuls. Si $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ et $b=p_1^{\beta_1}\dots p_k^{\beta_k}$ où les p_i sont des premiers distincts 2 à 2, $\alpha_i,\beta_i\in\mathbb{N}$, alors $a|b\Longleftrightarrow \forall i\in \llbracket 1,k \rrbracket, \alpha_i\leqslant \beta_i$ $a\land b=\prod_{i=1}^k p_i^{\min(\alpha_i,\beta_i)}$ et $a\lor b=\prod_{i=1}^k p_i^{\max(\alpha_i,\beta_i)}$

Ce qui peut aussi s'écrire :

Corollaire - Liste des diviseurs, avec la valuation

$$\begin{aligned} a|b &\Longleftrightarrow \forall p \text{ premier }, v_p(a) \leqslant v_p(b) \\ \text{Et } \forall p \in \mathscr{P}, \left\{ \begin{array}{l} v_p(a \land b) = \min(v_p(a), v_p(b)) \\ v_p(a \lor b) = \max(v_p(a), v_p(b)) \end{array} \right. \end{aligned}$$

Leçon 45 - Nombres premiers

⇒ Valuations
p-adique

⇒ Petit Ferma

- 1. Problèmes
- Théorèmes d'Euclide
 - .1. Definition
- 2.2. Théorème fondemental
- 3. L'ensemble des nombres premiers
- 3.1. Ensemble infini
- 3.2. Crible d Eratostne
- 4. Valuation (p-adique)
- 4.1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- premiers
 - .4. Formule de Legend
- 5. Petit Fermat
- 5.1. Motivations
- 5.2. Enoncé et ap

Factorisations

Application Algorithme de recherche du PGCD

Leçon 45 - Nombres premiers

⇒ Petit Fermat

1. Problèmes

- 2. Théorèmes d'Euclide
 - uclide
- 2.2. Lemmes d'Euclide
- 3. L'ensemble des
- ombres premier
- 1. Ensemble infini
- .2. Crible d'Eratosthèr
- . Valuation p-adique)
- Fonction valuation
- 4.2. Morphisme (de monoïde)
 4.3. Factorisation en produit de
- premiers
 - l. Formule de Legend

Petit Ferma

- 5.1. Motivations
- 5.2. Enonce e
 - Démonstrations

Factorisations

Application Algorithme de recherche du PGCD **Démonstration**

Leçon 45 - Nombres premiers

- Nombres p

- Botit Format

1. Problèmes

2 Tháoràmas

'Euclide

2 Lammas d'Euclida

2.3. Théorème fondamental

 L'ensemble des nombres premiers

.1. Ensemble infini

.2. Crible d'Eratosthèn

. Valuation

.1. Fonction valuat

2. Morohisme (de monoïde)

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de

premiers

l. Formule de Legend

5. Petit Fermat

5.1. Motivations

5.2. Enoncé el

3. Démonstrations

Factorisations

Application Algorithme de recherche du PGCD **Démonstration**

Exercice

Soit $n \in \mathbb{N}^*$. Donner une expression de $\operatorname{card}(\mathcal{D}(n))$, utilisant les valuations $v_p(n)$.

Leçon 45 - Nombres premiers

Valuations

⇒ Petit Fermat

- 1. Problèmes
- Théorèmes d'Euclide
 - Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - 1. Ensemble infir
 - 3.2. Crible d'Eratosthè
 - Valuation valuation
 - .1. Fonction valuatio
 - Morphisme (de monoïde)
 - 4.3. Factorisation en produit de
 - Formule de Legendr
- 5. Petit Fermat
 - .1. Motivations
 - 2. Enoncé et ap

⇒ Nombres premiers
\Rightarrow Valuations p -adique
⇒ Petit théorème de F

1. Problèmes

- 2. Théorèmes d'Euclide
- 3. L'ensemble des nombres premiers
- 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers

Fermat

- 4.4. Formule de Legendre
- Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

4.4. Formule de Legendre

Formule de Legendre, sous forme d'exercice

Exercice

Soit p un nombre premier.

Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ (la somme étant en réalité finie).

On pourra s'intéresser aux ensembles $N_a = \{k \in \mathbb{N}_n \mid p^a | k\}$.

Lecon 45 - Nombres

- 1. Problèmes

- 4 Valuation

- 4.4. Formule de Legendre

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers
 - 5.1. Motivations

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

Motivations

Heuristique. Décomposable vs. décomposition

L'analyse de la primalité d'un nombre n, entier, peut déboucher sur 4 questions de complexité différente :

- 1. Prouver que n n'est pas premier
- 2. Si n n'est pas premier, le décomposer
- 3. Garantir avec un risque d'erreur faible que n est premier
- 4. Certifier que *n* est premier.

Cela semble comparable, mais le petit théorème de Fermat permet de répondre « aisément »aux questions 1. et 3. Les deux autres questions qui semblent équivalentes sont bien plus compliquées. . .

Leçon 45 - Nombres premiers

Valuations
-adique

⇒ Petit Ferma

- Problèmes
- Théorèmes d'Euclide
- 2.1. Définit
- 2.2. Théorème fondemental
- L'ensemble des
- nombres premiers
- 3.2. Crible d'Eratosthène
- 4. Valuation
- p-adique)
- I.1. Fonction valuation
- 4.2. Morphisme (de monoîde)
- emiers
- 4. Formule de Legen
- 5. Petit Fermat
- 5.1. Motivations
- 2. Enonce et appi

Origine du théorème

Remarque Obtenir des nombres premiers

Leçon 45 - Nombres premiers

- Nombres p

> Potit Format

1. Problèmes

.....

- d'Euclide
- 1. Définition
- .2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- L'ensemble des nombres premiers
 - Ensemble infini
- .2. Crible d'Eratosthèn
- Valuation valuation
- .1. Fonction valuat
- 4.2 Morohisme (de monoïde)
- 4.2. Morphisme (de monoïde)
- premiers
- .4. Formule de Legeno
- 5. Petit Fermai
- 5.1. Motivations
- ----

Origine du théorème

Remarque Obtenir des nombres premiers **Analyse** Pour Fermat?

Pierre de Fermat était fasciné par la proposition de Diophante : « $si\ s(n)=1+2+\cdots+2^{n-1}$ est un nombre premier, alors $2^{n-1}s(n)$ est un nombre parfait »

Leçon 45 - Nombres premiers

⇒ Valuation

⇒ Petit Fermat

- 1. Problèmes
- 2. Théorèmes d'Euclide
- 2.1. Défini
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - 1. Ensemble infini
- 3.2. Crible d'Eratosthè
- 4. Valuation
 - -adique)
- 4.1. Fonction valuation
- I.2. Morphisme (de monoïde)
- 4.3. Factorisation en produit
- 4. Formule de Legendr
- 5 Petit Fermat
- 5.1. Motivations
- 5.2. Enoncé et a
 - . Démonstrations

Origine du théorème

Remarque Obtenir des nombres premiers

Analyse Pour Fermat?

Pierre de Fermat était fasciné par la proposition de Diophante : « $sis(n) = 1 + 2 + \cdots + 2^{n-1}$ est un nombre premier, alors

 $2^{n-1}s(n)$ est un nombre parfait »

Un seul candidat : $(2^{37} - 1) \times 2^{36}$. « Or $2^{37} - 1$ n'est pas

premier »FERMAT...

Leçon 45 - Nombres premiers

→ Valuations

⇒ Petit Fermat

1. Problèmes

Théorèmes d'Euclide

2.1. Defin

2.2. Lemmes d'Euclide

2.3. Théorème fondamental

 L'ensemble des nombres premiers

3.1. Ensemble infini

3.2. Crible d'Eratosthé

4 Valuation

p-adique)
4.1. Fonction valuation

4.1. Fonction valuation
4.3. Morphisms (do manaido)

4.2. Morphisme (de monoïde)

oremiers

1.4. Formule de Legend

5. Petit Fermat

5.1. Motivations

.2. Enonce et appi

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
- 3. L'ensemble des nombres premiers
- 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base p)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
- Garantir que des nombres sont premiers

 - 5.2. Enoncé et applications

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

Enoncé

Théorème - Petit théorème de Fermat (1640)

Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$. Si $n \land p = 1$ (i.e. p ne divise pas n), alors $n^{p-1} \equiv 1[p]$ Leçon 45 - Nombres premiers

→ Valuations

⇒ Petit Ferma

- 1. Problèmes
- Théorèmes
 Euclide
- 1 Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamenta
- 3. L'ensemble des nombres premiers
 - .1. Ensemble infini
- 3.2. Crible d'Eratosthè
 - Valuation valuation
- 4.1. Fonction valua
- 4.1. I Oriciori valuaziori
 4.2 Morobiomo (do monoido)
- 4.3. Factorisation en produit o
- .4. Formule de Legendre
- 5 Petit Fermat
- 5.1. Motivations
- 5.2. Enoncé et a
 - Démonstrations

Théorème - Petit théorème de Fermat (1640)

Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$. Si $n \wedge p = 1$ (i.e. p ne divise pas n), alors $n^{p-1} \equiv 1[p]$

Savoir-faire. Comment exploiter ce théorème?

Il y a deux façons d'exploiter ce théorème pour un nombre N:

- Trouver une factorisation (plus exactement un facteur premier) du nombre N de la forme $a^n - 1$ (voir l'application qui suit)
- ightharpoonup Montrer que le nombre N est probablement premier ; dans ce cas N joue le rôle de p (voir la remarque : nombre de Carmichaël)

Et les méthodes vues dans le petit contrôle de calcul...

Lecon 45 - Nombres

- 1. Problèmes
- 2. Théorèmes

- 4 Valuation

Applications

Application $2^{37} - 1$ est-il premier?

Leçon 45 - Nombres premiers

⇒ Petit Fermat

Problèmes

2. Théorèmes d'Euclide

- l'Euclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - 3.1. Ensemble infini
 - .2. Crible d'Eratosthèn

Valuation -adique)

- .1. Fonction valuat
- 2 Morohiema (da monoida)
- 4.2. Morphisme (de monoide)
- premiers
- Formule de Legend

5. Petit Fermat

- 5.1. Motivations
- 5.2. Enonce et applica

Applications

Application $2^{37} - 1$ est-il premier?

Remarque Réciproque? Nombre de Carmichaël

Leçon 45 - Nombres premiers

→ Valuations

⇒ Petit Fermat

1. Problèmes

Théorèmes d'Euclide

2.1 Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

ombres premier

.1. Ensemble infini

8.2. Crible d'Eratosthe

Valuation o-adique)

- 4.1. Fonction valua
- I.2. Morphisme (de monoïde)
- 4.3. Factorisation en produit d
 - I. Formule de Legendre

4.4. Formule de Legendre

E t Marianian

5.1. Motivation

5.E. Enonce et a

- ⇒ Nombres premiers \Rightarrow Valuations p-adique ⇒ Petit théorème de Fermat.
 - 1. Problèmes
 - 2. Théorèmes d'Euclide
 - 3. L'ensemble des nombres premiers
 - 4. Valuation (*p*-adique)
 - 4.1. Fonction valuation (en base *p*)
 - 4.2. Morphisme (de monoïde)
 - 4.3. Factorisation en produit de premiers
 - 4.4. Formule de Legendre
 - Garantir que des nombres sont premiers

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

Nous ferons plusieurs démonstrations

Leçon 45 - Nombres premiers

⇒ Nombres p

⇒ Valuations p-adique

⇒ Petit Fermat

1. Problèmes

Théorèmes Euclide

- zuciide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamenta
- 3. L'ensemble des nombres premiers
 - 3.1. Ensemble infini
- 3.2. Crible d'Eratosthè

Valuation -adique)

- .1. Fonction valuati
- 1.2 Morohisme (de monoide)
- 4.2. Horprisation on produit
 - 1.4 Formule de Lenend
 - .4. Formule de Legendr

5. Petit Fermat

- 5.1. Motivatio
- 5.2. Ellonce el
- 5.3. Démonstrations

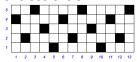
Nous ferons plusieurs démonstrations

Heuristique- Illustration de la démonstration

Dans le cas de p = 13 et n = 31.

On a alors $n \equiv 5[13]$ et donc $kn \equiv r_k$ se voit sur le carrelage (a = p = 13, b = 5).

On remarque alors que tous les restes sont obtenus, et une et une seule fois



Et les tables de multiplications du problème 53

Leçon 45 - Nombres premiers

→ Valuations p-adique

⇒ Petit Ferma

1. Problèmes

2. Théorème:

2.1. Définition

2. Lemmes d'Eucli

2.3. Théorème fondamental

L'ensemble des nombres premiers

3.1. Ensemble infini

3.2. Crible d'Eratosthé

4. Valuation (p-adique)

4.1. Fonction valuation

4.2. Morphisme (de monoîde)

premiers

.4. Formule de Legendr

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et a

Démonstrations

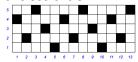
Nous ferons plusieurs démonstrations

Heuristique- Illustration de la démonstration

Dans le cas de p = 13 et n = 31.

On a alors $n \equiv 5[13]$ et donc $kn \equiv r_k$ se voit sur le carrelage (a = p = 13, b = 5).

On remarque alors que tous les restes sont obtenus, et une et une seule fois



Et les tables de multiplications du problème 53

Démonstration

Leçon 45 - Nombres premiers

⇒ Valuation

⇒ Petit Ferma

- 1. Problèmes
- 2. Théorème: d'Euclide
 - .1. Definition
- 2.2. Théorème fondamental
- 3. L'ensemble des
- 3.1. Ensemble infini
- 3.2. Crible d'Eratosthèr
- 4. Valuation (p-adique)
- 4.1. Fonction valuation
- 4.2. Morphisme (de monoîde)
- premiers
- 4. Formule de Legend
- 5. Petit Fermat
- .1. Motivations
- 5.2. Enoncé et
 - . Démonstrations

Autres démonstrations

Leçon 45 - Nombres premiers

⇒ Nombres p

> Valuation -adique

⇒ Petit Fermat

Problèmes

- 2. Théorèmes d'Euclide
 - =uclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamenta
- 3. L'ensemble des nombres premiers
- 3.1. Ensemble infini
- 3.2. Crible d'Eratosthè
- I. Valuation p-adique)
- .1. Fonction valuat
- 2 Morohieme (de monoide)
- .2. Morphisme (de monoïde)
- premiers
 - 4. Formule de Legendr
- 5. Petit Fermat
- 5.1. Motivation
- 5.2. Enoncé e
- 5.3. Démonstrations

Autres démonstrations

Voici la première démonstration historique d'Euler et probablement de Leibniz :

Exercice

Considérons p, un nombre premier.

- 1. Montrer que pour tout $k \in [1, p-1], p \mid {p \choose k}$.
- 2. Montrer que pour tout $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p[p]$
- En déduire le petit théorème de Fermat.

Lecon 45 - Nombres premiers

1 Problèmes

4 Valuation

Autres démonstrations

Voici la première démonstration historique d'Euler et probablement de Leibniz :

Exercice

Considérons p, un nombre premier.

- 1. Montrer que pour tout $k \in [1, p-1], p | {p \choose k}$.
- 2. Montrer que pour tout $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p[p]$
- 3. En déduire le petit théorème de Fermat.

Remarque Morphisme de Froebenius :

Si p est premier alors $(a+b)^p \equiv a^p + b^p[p]$.

Donc $x \mapsto x^p$ est un endomorphisme du corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Leçon 45 - Nombres premiers

⇒ Valuations
p-adique

⇒ Petit Fermat

- 1. Problèmes
- 2. Théorèmes l'Euclide
- 2.1. Défin
- .2. Lemmes d'Euclic
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
 - nnbres premie 1. Ensemble infini
- 3.2. Crible d'Eratosthè
- 4. Valuation
- 4.1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- 4.3. Factorisation en produit
- .4. Formule de Legeno
- I.4. Formule de Legend
- 6. Petit Fermat
- .1. Motivations
- 5.2. EHOHOU ULAJ

Autres démonstrations

Leçon 45 - Nombres premiers

- Nombres pre

⇒ Petit Fermat

. Problèmes

- Théorèmes d'Euclide
- 1 Définition
- 2.2. Lemmes d'Euclide
- 0 11----------
- nombres premiers
- 3.1. Ensemble Infini
- 3.2. Crible d'Eratosthèr
- Valuation p-adique)
- 4.1. Fonction valuation
- 2 Morobiema (da monoida
- 4.2. Morphisme (de monoïde)
- premiers
- l.4. Formule de Legend

Petit Ferma

- 5.1. Motivatio
- 5.2. Enoncé e
- 5.3. Démonstrations

Démonstrations

Autres démonstrations

Exercice

Par double dénombrement

Leçon 45 - Nombres premiers

⇒ Nombres (

⇒ Valuatio
p-adique

⇒ Petit Fermat

1. Problèmes

Théorème d'Euclide

- Lucilue
- 2.2. Lemmes d'Euclide
- 3. L'ensemble des
 - .1. Ensemble infini
 - .2. Crible d'Eratosthèn

Valuation

- 4.1. Fonction value
- 2 Morobiema (da monoida)
- 4.3 Factorisation en produit d
- l.4. Formule de Legend

5.1. Motivation

- o. i. mouvation
- 5.3. Démonstrations

Démonstrations

Autres démonstrations

Exercice

Par double dénombrement

Avec la formule de Lagrange :

Exercice

Soit $p \in \mathcal{P}$. Soit $n \in \mathbb{Z}$. Supposons que p ne divise pas n. Notons r = n%p.

- 1. On note $G = ([1, p-1]], \times)$. Montrer que G est un groupe (fini).
- 2. Montrer qu'il existe $k \in \mathbb{N}$ tel que $r^k \equiv \mathbb{I}[p]$. On note $k_0 = \min\{k \in \mathbb{N} \mid r^k \equiv \mathbb{I}[p]\}.$
- 3. Montrer que \mathcal{R} définie par : $a\mathcal{R}b$ ssi $\exists k \in \mathbb{Z}$ tel que $a = r^k b$ est une relation d'équivalence.
- 4. Quel est la taille de chacun des classes d'équivalence?
- 5. On note h, le nombre de classe d'équivalence. Montrer que $p-1=k_0\times h$. En déduire la valeur de r^{p-1} , puis le petit théorème de Fermat.

Lecon 45 - Nombres

1 Problèmes

4 Valuation

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat

Leçon 45 - Nombres premiers

- Voluntiana

- 1. Problèmes
 - . Théorèmes 'Euclide
 - =uclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- B. L'ensemble des nombres premiers
- Ensemble infini
- 3.2. Crible d'Eratosthè
- Valuation
-
- 0 Manabiana (da manafida)
- .2. Morphisme (de monoïde)
- premiers
- Formule de Legend
- 5 Petit Fermat
 - 5.1. Motivation
 - 5.2. Enoncé et
 - . Démonstrations

Objectifs

- ⇒ Nombres premiers
 - Définition : p est premier ssi $\mathcal{D}(p) = \{-p, -1, 1, p\}$ et $|p| \neq 1$

Lecon 45 - Nombres premiers

- 1. Problèmes

Objectifs

- ⇒ Nombres premiers
 - ▶ Définition : p est premier ssi $\mathcal{D}(p) = \{-p, -1, 1, p\}$ et $|p| \neq 1$
 - Tout nombre s'écrit de manière unique comme un produit de nombre premier.

Leçon 45 - Nombres premiers

→ Nollibres p

p danque

- 1. Problèmes
- 2. Théorèmes l'Euclide
- 2.1. Définiti
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- L'ensemble des nombres premiers
- 3.1. Ensemble infini
- 3.2. Crible d'Eratostne
- . Valuation
- 4.1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- 4.3. Factorisation en produit d
 - 4. Formule de Legendr
 - .4. Formule de Legendre
- E 4 Marianiana
- 5.1. Motivations
 - Dámanatrationa

Objectifs

- ⇒ Nombres premiers
 - ▶ Définition : p est premier ssi $\mathcal{D}(p) = \{-p, -1, 1, p\}$ et $|p| \neq 1$
 - Tout nombre s'écrit de manière unique comme un produit de nombre premier.
 - Ensemble dénombrable des nombres premiers

Leçon 45 - Nombres premiers

⇒ Nombres p

Valuationsadique

- 1. Problèmes
- 2. Théorèmes l'Euclide
- 2.1. Définition
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- 3. L'ensemble des nombres premiers
- 3.1. Ensemble infini 3.2. Crible d'Eratoethè
- 5.2. Office a Liatosti
- . Valuation
- .1. Fonction valuation
- 4.1. I Orichori varidation
 4.2 Morrobieme (de monoide)
- 4.2. Morphisme (de monoide)

 4.3. Factorisation en produit d
 - .4. Formule de Legendr
- - 5.1. Motivations
- 5.2. Enoncé et
 - I. Démonstrations

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat

Leçon 45 - Nombres premiers

- Voluntiana

- 1. Problèmes
 - . Théorèmes 'Euclide
 - =uclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- B. L'ensemble des nombres premiers
- Ensemble infini
- 3.2. Crible d'Eratosthè
- Valuation
-
- 0 Manabiana (da manafida)
- .2. Morphisme (de monoïde)
- premiers
- Formule de Legend
- 5 Petit Fermat
 - 5.1. Motivation
 - 5.2. Enoncé et
 - . Démonstrations

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
 - Décomposition de n : quelle puissance p-ième ?

Leçon 45 - Nombres premiers

→ Molilibres F

-adique

⇒ Petit Fermat

1. Problèmes

2. Théorèmes d'Euclide

- Lacinae
- 2.2. Lemmes d'Euclide
- 2 L'ancomble des
- ombres premier
- 3.2 Crible d'Eretneti
- Crible d Eratostrie

4. Valuation

- 4.1. Fonction valuation
- 4.2. Morphisme (de monoïde)
- 4.3. Factorisation en produit d
 - .4. Formule de Legendre
- 4.4. Formule de Legendi

5. Petit Ferma

- 5.1. Motivation
- 5.2. Enonce et a

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
 - Décomposition de n : quelle puissance p-ième ?
 - Propriété logarithmique : $v_p(ab) = v_p(a) + v_p(b)$

Leçon 45 - Nombres premiers

→ valuation -adique

⇒ Petit Fermat

1. Problèmes

2. Théorèmes

Euclide

2.2. Lemmes d'Euclide

. L'ensemble des

.1. Ensemble infini

2. Crible d'Erstoethà

3.2. Crible d'Eratosthèr

.1. Fonction valuatio

4.1. Poncilon valuation

4.2 Morphisma (de monoida

4.2. Morphisme (de monoîde)

premiers

4. Formule de Legendr

Petit Fermat

5.1. Motivatio

5.2. Enoncé et a

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation *p*-adique
 - Décomposition de n: quelle puissance p-ième?
 - Propriété logarithmique : $v_p(ab) = v_p(a) + v_p(b)$
 - Formule de Legendre

Lecon 45 - Nombres premiers

1. Problèmes

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat

Leçon 45 - Nombres premiers

- Voluntiana

- 1. Problèmes
 - . Théorèmes 'Euclide
 - =uclide
- 2.2. Lemmes d'Euclide
- 2.3. Théorème fondamental
- B. L'ensemble des nombres premiers
- Ensemble infini
- 3.2. Crible d'Eratosthè
- Valuation
-
- 0 Manabiana (da manafida)
- .2. Morphisme (de monoïde)
- premiers
- Formule de Legend
- 5 Petit Fermat
 - 5.1. Motivation
 - 5.2. Enoncé et
 - . Démonstrations

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat
 - Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.

Lecon 45 - Nombres premiers

1. Problèmes

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat
 - Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.
 - Si $n \wedge p = 1$ (i.e. p ne divise pas n), alors $n^{p-1} \equiv 1[p]$

Lecon 45 - Nombres premiers

- 1. Problèmes

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat
 - Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.
 - Si $n \wedge p = 1$ (i.e. p ne divise pas n), alors $n^{p-1} \equiv 1[p]$
 - Utilisations :
 - Montrer qu'un nombre n'est pas premier (ou probablement pas)
 - Factoriser un grand nombre N (en réfléchissant sur les puissances).

Leçon 45 - Nombres premiers

⇒ Valuation

⇒ Petit Fermat

1. Problèmes

Théorème d'Euclide

.1. Definition

2.3. Théorème fondamental

3. L'ensemble des nombres premiers

3.1. Ensemble infini
3.2 Crible d'Eratoeth

3.2. Crible d'Eratosth

4. Valuation (p-adique)

4.1. Fonction valuation

4.1. Fonction valuation
4.2 Morphisms (de monoide)

4.3. Factorisation en produi

prenners 4.4. Eormulo do Logand

4.4. Formule de Legeno

5. Felli Fellik

.1. Motivations

e. Eriorice et applic

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat
 - Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.
 - Si $n \wedge p = 1$ (i.e. p ne divise pas n), alors $n^{p-1} \equiv 1[p]$
 - Utilisations :
 - Montrer qu'un nombre n'est pas premier (ou probablement pas)
 - Factoriser un grand nombre N (en réfléchissant sur les puissances).
 - Plusieurs démonstrations :
 - ► On exploite la table $\times a$ (bijective) sur le groupe $\left(\frac{Z}{pZ}^*, \times\right)$
 - On crée/exploite le morphisme de Froebenius sur le corps $\frac{\mathbb{Z}}{n\mathbb{Z}}$
 - ▶ On étudie la suite (a^k) est on voit comment elle partitionne le groupe $\left(\frac{Z}{p\mathbb{Z}}^*,\times\right)$ en classes d'équivalence de même cardinal (Méthode de Lagrange).

Leçon 45 - Nombres premiers

⇒ Valuation

⇒ Petit Fermat

1. Problèmes

2. Theoremes d'Euclide

1. Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

Ensemble infini
 Crible d'Eratosthé

Valuation

Valuation
 (p-adique)

4.1. Fonction valuation

4.2. Morphisme (de monoîde)

remiers

4. Formule de Lege

5. Petit Fermat

5.1. Motivations

. Enoncé et applica

Objectifs

- ⇒ Nombres premiers
- \Rightarrow Valuation p-adique
- ⇒ « Petit » théorème de Fermat

Pour la prochaine fois

- Lecture du cours : chapitre 9 : Calcul matriciel
- Exercice N°316 & 320
- ► TD de jeudi

8h-10h : N°313, 318, 317, 203, 206

10h-12h: N°314, 319, 321, 240, 207

Leçon 45 - Nombres premiers

→ Valuation
a-adique

⇒ Petit Ferma

1. Problèmes

2. Théorèmes d'Euclide

2.1 Définition

2.2. Lemmes d'Euclide

3. L'ensemble des

nombres premie

3.1. Ensemble Infin 3.2. Crible d'Eratos

Valuation (p-adique)

4.1. Fonction valuat

4.2. Morphisme (de monoïde)

v.s. racionsation en pro premiers

4.4. Formule de Legendi

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et