Leçon 47 - Nombres premiers

12 décembre 2025

⇒ Nombres premiers

⇒ 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. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

5.2. Enoncé et applications

5.3. Démonstrations

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

Problèmes

Problème - Produit de premiers

Problèmes

Problème - Produit de premiers

Problème - Constructions de cours

Problèmes

Problème - Produit de premiers

Problème - Constructions de cours

Problème - Fonctions arithmétiques

⇒ Nombres premiers

⇒ 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. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

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.

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 $\mathscr{P}$, l'ensemble des nombres premiers.

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

Lemme de Gauss pour les premiers

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

Lemme de Gauss pour les premiers

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.

Lemme de Gauss pour les premiers

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

Lemme de Gauss pour les premiers

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 $p \in \mathscr{P}$ 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 $b = 4$.

Existence

Théorème -

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

Existence

Théorème -

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

Démonstration

Existence

Théorème -

Tout entier naturel $n \geqslant 2$ 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.

Existence

Théorème -

Tout entier naturel $n \geqslant 2$ 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

⇒ Nombres premiers

⇒ 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

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de premiers

4.4. Formule de Legendre

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers

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

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.

Théorème fondamental de l'arithmétique

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers

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

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

Théorème d'Euclide

Proposition - (Second) théorème d'Euclide

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

Théorème d'Euclide

Proposition - (Second) théorème d'Euclide

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

Démonstration

Description énumérative de $\mathscr{P}$

Remarque Ensemble dénombrable

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.

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} ?

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

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

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.

Crible d'Eratosthène

Python - Crible d'Eratosthène

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

Culture

Remarque Conjectures

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

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

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

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

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...).

Evaluation de p_{1000}

Exercice

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

⇒ Nombres premiers

⇒ 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

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de premiers

4.4. Formule de Legendre

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

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 $v_p(n)$.

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 $v_p(n)$.

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

Savoir-faire. Caractérisation

$p^k | a \iff v_p(a) \geqslant k$
$(a = p^h q \text{ et } p \wedge q = 1) \iff v_p(a) = h$

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 $v_p(n)$.

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

Savoir-faire. Caractérisation

$p^k | a \iff v_p(a) \geqslant k$
$(a = p^h q \text{ et } p \wedge q = 1) \iff v_p(a) = h$

Démonstration

Réécriture

Exercice

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

Réécriture

Exercice

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

Remarque Réécriture du théorème fondamental de l'arithmétique

⇒ Nombres premiers

⇒ 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

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de premiers

4.4. Formule de Legendre

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

Propriété logarithmique

Proposition - Valuation, fonction logarithmique

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

Propriété logarithmique

Proposition - Valuation, fonction logarithmique

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

Démonstration

⇒ Nombres premiers

⇒ 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

4.2. Morphisme (de monoïde)

4.3. Factorisation en produit de premiers

4.4. Formule de Legendre

5. Petit Fermat

5.1. Motivations

5.2. Enoncé et applications

5.3. Démonstrations

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

$$a|b \iff \forall i \in [\![1, k]\!],\ \alpha_i \leqslant \beta_i$$

$$a \wedge b = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)} \text{ et } a \vee b = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

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

$$a|b \iff \forall i \in [\![1,k]\!],\ \alpha_i \leqslant \beta_i$$

$$a \wedge b = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \text{ et } a \vee b = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}$$

Ce qui peut aussi s'écrire :

Corollaire - Liste des diviseurs, avec la valuation

$$a|b \iff \forall p \text{ premier }, v_p(a) \leqslant v_p(b)$$

$$\text{Et } \forall p \in \mathscr{P}, \begin{cases} v_p(a \wedge b) = \min(v_p(a), v_p(b)) \\ v_p(a \vee b) = \max(v_p(a), v_p(b)) \end{cases}$$

Factorisations

Application Algorithme de recherche du PGCD

Factorisations

Application Algorithme de recherche du PGCD

Démonstration

Factorisations

Application Algorithme de recherche du PGCD

Démonstration

Exercice

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

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

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 $N_a = \{k \in \mathbb{N}_n \mid p^a | k\}$.

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

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. . .

Origine du théorème

Remarque Obtenir des nombres premiers

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 »*

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* »

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

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

Enoncé

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 $n^{p-1} \equiv 1[p]$

Enoncé

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)
- 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. . .

Applications

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

Applications

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

Remarque Réciproque ? Nombre de Carmichaël

⇒ Nombres premiers

⇒ Valuations p-adique

⇒ Petit théorème de Fermat

Démonstrations

Nous ferons plusieurs démonstrations

Démonstrations

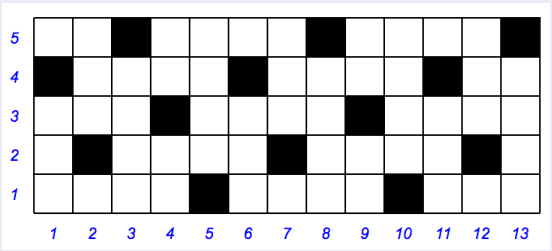
Nous ferons plusieurs démonstrations

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

Démonstrations

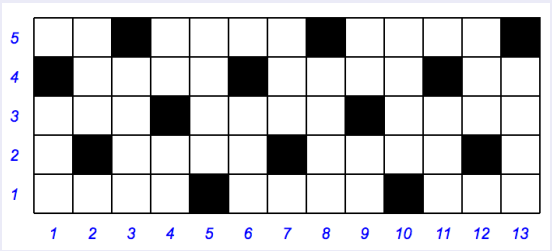
Nous ferons plusieurs démonstrations

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

Démonstrations

Autres démonstrations

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 $k \in [\![1, p-1]\!]$, $p | \binom{p}{k}$.
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.

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 $k \in [\![1, p-1]\!]$, $p | \binom{p}{k}$.
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 $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Démonstrations

Autres démonstrations

Démonstrations

Autres démonstrations

Exercice

Par double dénombrement

Démonstrations

Autres démonstrations

Exercice

Par double dénombrement

Avec la formule de Lagrange :

Exercice

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

1. On note $G = (\llbracket 1, p-1 \rrbracket, \times)$. Montrer que G est un groupe (fini).
2. Montrer qu'il existe $k \in \mathbb{N}$ tel que $r^k \equiv 1[p]$. On note $k_0 = \min\{k \in \mathbb{N} \mid r^k \equiv 1[p]\}$.
3. Montrer que $\mathscr{R}$ définie par : $a \mathscr{R} b$ 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.

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

⇒ « Petit » théorème de Fermat

Conclusion

Objectifs

⇒ Nombres premiers

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

Conclusion

Objectifs

⇒ Nombres premiers

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

Conclusion

Objectifs

⇒ Nombres premiers

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

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

⇒ « Petit » théorème de Fermat

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

- Décomposition de n : quelle puissance p-ième ?

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

- Décomposition de n : quelle puissance p-ième ?
- Propriété logarithmique : $v_p(ab) = v_p(a) + v_p(b)$

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

- Décomposition de n : quelle puissance p-ième ?
- Propriété logarithmique : $v_p(ab) = v_p(a) + v_p(b)$
- Formule de Legendre

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

⇒ « Petit » théorème de Fermat

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

⇒ « Petit » théorème de Fermat

- Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.

Conclusion

Objectifs

⇒ Nombres premiers

⇒ 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 $n^{p-1} \equiv 1[p]$

Conclusion

Objectifs

⇒ Nombres premiers

⇒ 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).

Conclusion

Objectifs

⇒ Nombres premiers

⇒ 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 $\left(\frac{Z}{p\mathbb{Z}}^*, \times\right)$
  - On crée/exploite le morphisme de Froebenius sur le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$
  - 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).

Conclusion

Objectifs

⇒ Nombres premiers

⇒ Valuation p-adique

⇒ « Petit » théorème de Fermat

Pour la prochaine fois

- Lecture du cours : chapitre 9 : Calcul matriciel
- Exercice N° 324, 325 & 327
- TD de jeudi
  8h-10h : N°329, 326 + matrices
  10h-12h : N°330, 332 + matrices