121 - Nombres premiers. Applications.

Références	[GOU_AGP], [Perrin], [Gozard], [M2M]
Section	Algèbre
Date	@12 février 2025
Statut leçon	Plan détaillé ok REF !
Enseignant	Lionel Fourquaux
Développements choisis	Entiers de Gauss et Théorèmes des deux carrés., Dirichlet faible et app Z/nZ
Nb choisis	2
Autres développements à case comme item	Loi de réciprocité quadratique, Ore / Frattini
Développements	Entiers de Gauss et Théorèmes des deux carrés., Loi de réciprocité quadratique

Rapport de Jury

Le sujet de cette leçon est très vaste. Elle doit donc être abordée en faisant des choix qui devront être clairement motivés. On attend une étude purement interne à l'arithmétique
des entiers, avec des applications dans différents domaines : théorie des corps finis, théorie des groupes, arithmétique des polynômes, cryptographie, etc. On peut définir certaines fonctions importantes en arithmétique, les relier aux nombres premiers et illustrer leurs utilisations. Il est recommandé de s'intéresser aux aspects algorithmiques du sujet (tests de primalité). La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour
résoudre des problèmes arithmétiques simples. La répartition des nombres premiers doit être évoquée : certains résultats sont accessibles dans le cadre du programme du concours, d'autres peuvent être admis et cités pour leur importance culturelle.

Introduction

→ briques élémentaires des entiers, Idée : on aime fragmenter les choses pour revenir au problème initial.

→ On les retrouve aussi dans d'autres sciences, comme en cryptographie, où la sécurité de
nombreux protocoles découlent de la difficulté à les trouver et à factoriser un entier quel-
conque.

Plans

▼ ***Plan***

- Définition
- existe une infinité

I. Théo fondamental et conséquences

1. Théorème et premières csq
2. Indicatrice d'Euler et chiffrement RSA
3. Théorème des deux carrés
4. Nombres de Fermat et constructibilité

II. Répartition/recherche des nombres premiers

1. Recherche de nbrs premiers
2. Répartition des nombres premiers

III. Particularités des nombres premiers en algèbre

1. Réduction de polynômes
2. p-groupes
3. Corps finis

▼ ***Plan détaillé***

- def nbr premier et notation ensemble des nombres premiers
- prop: existe une inifinité

▼ I.1. Théo fonda et premières csq

- théo fondamental de l'arithmétique + ex (si veut peut parler fonction mobius qui se définit avec ça vu qu'en parle dans rapport)
- Ex racine de 2 non rationnel
- somme des 1/p diverge, où ? Et app Borel Cantelli
- indicatrice d'Euler d'un nombre n quelconque

° Valuation/pgcd

- def valuation p-adique
- def pgcd et ppcm avec valuation + ex

▼ I. 2. Indicatrice d'EUler et RSA

- def indicatrice d'Euler + phi(p)=p-1 + expression phi(n) avec décomposition
- petit théo Fermat= a^p-1 \equiv 1 mod p
- Chiffrement RSA

▼ I. 3. Théorème des deux carrés

- les pptés nécessaire et DEV 1

▼ I.4. Nbr de fermat

- def nbr Fermat + constructibilité de polygones réguliers

▼ II. 1. Recherche de nombres premiers

- Crible d'Eratosthène + tableau en annexe si on a le temps
- test primalité avec nbr de Carmichael = primalité de Fermat ?
- (non primalité de Perrin)
- (Theo de Wilson dans la dernière partie)

▼ II. 2. Répartition des nbrs premiers

- def pi(n)
- il existe un nbr premier entre n et 2n
- borne sur pi(n)
- pi(n) equivalent n/ln n
- dirichelt faible DEV2
- dirichlet fort

▼ III. 1. Réduction de polynômes

- Eisenstein
- critère de réduction
- Ex de l'irreductibilite des polynômes cyclotomiques (on réduit modulo p)

▼ III.2. Théorie des groupes

° p groupes

- def p groupe
- Lagrange + conséquence de si groupe d'ordre premier
- prop equation au classe pour p groupe
- app: centre p groupe non trivial
- csq: G d'ordre p^2 est abélien
- lemme: tout sgrp maximal d'un p groupe est d'indice p
- thme Frattini: toute fg d'un p groupe au sens de l'inclusion st de même cardinal
- c-ex Z/6Z et {2,3}/{1}

°p Sylow

- def p sylow
- lemme Card(GLn(Fq)) qu'on factorise
- lemme 5.5 (Perrrin)
- thm 1
- thm2
- Cas n=6 dans Aut(Sn)

▼ III.3. Corps finis

- Résultat sur les corps finis (caractéristique p ⇒ p^n, Frobenius endomorphisme de corps,
- Carrés dans les corps finis
- Thm de Wilson: n est premier ssi (n-1)! \equiv 1 mod n
- Loi de réciprocité quadratique
- Tout elmt de Fp est somme des deux carrés (lien avec dev !)