NOM : CHABAUD Prénom : Ulysse

Rouge entourez l'épreuve Bleu entourez le Jury A B C D E F

Sujet choisi : 121 - Nombres premiers, applications.

Autre sujet :

I - Arithmétique

Déf 1 : Un entier $p \geq 2$ est dit premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Prop 2 : L'ensemble $\mathcal{P}$ des nombres premiers est infini

Prop 3 : Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}$ avec $\neg(p \mid n)$, alors $p \wedge n = 1$

Prop 4 : $\forall n \in \mathbb{N}$, $n \geq 2 \Rightarrow \exists p \in \mathcal{P}$, $p \mid n$

Prop 5 : $p \in \mathcal{P} \Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ corps

Ex 6 : (Nombres de Fermat) $F_n = 2^{2^n} + 1$

$F_n \in \mathcal{P}$ pour $0 \leq n \leq 4$ mais pas F_5.

Prop 7 : Si $2^n + 1$ est premier, alors $\exists k \geq 0$, $n = 2^k$

Ex 8 : (Nombres de Mersenne) $M_p = 2^p - 1$, où $p \in \mathcal{P}$.

Si $a^n - 1$ est premier alors $a = 2$ et $n \in \mathcal{P}$,

mais $2^{11} - 1$ n'est pas premier.

Théorème 9 : (Petit théorème de Fermat) Si p est premier et si $a \in \mathbb{Z}$ n'est pas divisible par p alors $a^{p-1} \equiv 1 [p]$.

Rmq 10 : La réciproque est fausse, 561 par exemple.

Théorème 11 : (Wilson) $p \in \mathcal{P} \Leftrightarrow (p-1)! \equiv -1 \bmod p$.

Théorème 12 : (Crible d'Ératosthène) : $n \notin \mathcal{P} \Leftrightarrow \exists p \in \mathcal{P}$, $p \mid n$ et $p \leq \sqrt{n}$

Déf 13 : Un nombre non premier est dit composé.

II - Factorisation et divisibilité.

Théorème 14 : Tout entier naturel ≥ 2 admet une décomposition en facteurs premiers, unique à l'ordre près des facteurs

Ex 15 : $8 = 2^3$, $12 = 2^2 \times 3$, $33 = 3 \times 11$.

Prop 16 : Un entier naturel écrit en base 10 est divisible :

- par 2 ssi son dernier chiffre est pair,
- par 3 ssi la somme de ses chiffres l'est,
- par 5 ssi son dernier chiffre est 0 ou 5.

Déf 17 : Si $a \in \mathbb{N}^*$ et $p \in \mathcal{P}$, on appelle valuation p-adique de a et on note $v_p(a) = \max\{\alpha \in \mathbb{N} : p^\alpha \mid a\}$

Prop 18 : C'est l'exposant de p dans la décomposition de a en facteurs premiers : $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$

Prop 19 : $\forall a, b \in \mathbb{N}$, $a \mid b \Leftrightarrow \forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$

Prop 20 : $v_p(a \times b) = v_p(a) + v_p(b)$ et $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$

Application 21 : Existence du PGCD ($a \wedge b$) et du PPCM ($a \vee b$), tels que

- $\forall p \in \mathcal{P}$, $v_p(a \wedge b) = \min\{v_p(a), v_p(b)\}$
- $\forall p \in \mathcal{P}$, $v_p(a \vee b) = \max\{v_p(a), v_p(b)\}$

Application 22 : $(a \vee b) \times (a \wedge b) = a \times b$

Exo 23 : Résoudre $a^b = b^a$ dans $\mathbb{N}$.

Déf 24 : Une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{C}$ est dite multiplicative si pour tout $m, n \geq 1$ premiers entre eux, $f(mn) = f(m)f(n)$

Déf 25 : $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$, $n \longmapsto \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^*)$ est l'indicatrice d'Euler

Prop 26 : $\forall n \geq 1$, φ est multiplicative et telle que

$$\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

Prop 27 : De plus, $n = \sum_{d \mid n} \varphi(d)$

NOM : CHABAUD Prénom : Ulysse

Rouge entourez l'épreuve Bleu

Sujet choisi : 121 - Nombres premiers, applications.

Autre sujet : A B C D E F entourez le Jury

→ Un peu court en dev.

Application 28 : (codage RSA) Soit $p,q \in \mathcal{P}$ distincts et $c,d \in \mathbb{N}$ avec $cd \equiv 1 [\varphi(pq)]$, alors $\forall t \in \mathbb{Z}$, $t^{cd} \equiv t [pq]$

Ex 29 : $\sigma : n \longmapsto \sum_{d \mid n} d$ est également multiplicative.

Déf 30 : La fonction de Möbius définie par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré et $\mu(q_1 \cdots q_r) = (-1)^r$ si les q_i sont premiers distincts.

Prop 31 : μ est multiplicative.

DV1 → Application 32 : La probabilité r_n que deux entiers de $\{1, \dots, n\}$ soient premiers entre eux est

$$r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2$$

et tend vers $\frac{6}{\pi^2}$ lorsque n tend vers l'infini.

III - Répartition des nombres premiers

Exo 33 : $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge

Théorème 34 : (Progression arithmétique de Dirichlet) (Admis) Si $a, b \in \mathbb{N}^*$ sont premiers entre eux, alors il existe une infinité de nombres premiers de la forme $ak+b$.

Déf 35 : pour $n \in \mathbb{N}$, on note $\pi(n)$ le nombre de premiers $\leq n$.

Théorème 36 : (des Nombres Premiers) (admis) $\pi(n) \approx \frac{n}{\ln n}$

IV - Applications algébriques

Prop 37 : La caractéristique d'un corps fini est un nombre premier p et son cardinal une puissance de p.

Prop 38 : Si $\mathbb{K}$ est un corps de caractéristique p alors $\mathbb{K} \longrightarrow \mathbb{K}$, $x \longmapsto x^p$ est un homomorphisme, dit de Frobenius de $\mathbb{K}$.

Prop 39 : (Critère d'Eisenstein) Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$, si
- $\neg(p \mid a_n)$
- $p \mid a_0, \dots, a_{n-1}$
- $\neg(p^2 \mid a_0)$

alors P est irréductible dans $\mathbb{Q}[X]$.

Prop 40 : Un groupe d'ordre p est cyclique.

Prop 41 : Un groupe d'ordre p^2 est abélien.

Application 42 : Classification des groupes d'ordre pq ← DEV2

G un groupe fini d'ordre pq, où $p<q$ sont premiers
- Si q n'est pas congru à 1 modulo p, $G \simeq \mathbb{Z}/pq\mathbb{Z}$
- Si q est congru à 1 modulo p, alors soit $G \simeq \mathbb{Z}/p\mathbb{Z}$, soit G n'est pas commutatif et alors $G \simeq (\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$ avec $\theta \in \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}))$

Références : - F. Combes, Algèbre et géométrie | - Gourdon
- FGN, algèbre 1

DEV 1 : FGN, algèbre 1, p. 156

DEV 2 : F. Combes, Algèbre et géométrie, p. 94.

Rq: DVT

- Lev 1 : on utilise le fait que 0 est l'inv pour la compos° de... (qd on parle de la Rm)
  ↳ à mettre du le plan

Questions Plan

- Preuve de l'aspect de nombre premier
- Rq 10. cNm pour ces nbres ? ↳ nombre de Carmichael
- Thm 14. Cmt on montre l'unicité de la décomp° ?
  ↳ repose sr le thm de Gauss : $(a \mid bc) \wedge (b \wedge c = 1) \Rightarrow a \mid b$ ou $a \mid c$

  Et celui-ci se montre cmt ?
  ↳ ..

  Cmt on montre la prop 5 ?
  ↳

- Prop 26. Cmt on la trouve.
- Appli 28. Expliquer pquoi c'est efficace
- Qui a mq la $\sum 1/p$ div ? ↳ Euler
- Exple d'appli pr un polynome du critère d'Eisenstein (prop 39) ?
  ↳ $X^{16}+2$.

  Dem ?
  ↳ absurde $P = CB$. $C = X^d + p(\dots)$ $B = X^{d'} + p(\dots)$ terme cst : $d^2 1$..

  Utiliser ce critère pr mq $\frac{X^p - 1}{X-1}$ est irréductible dr $\mathbb{Q}[X]$
  ↳ idée : la transformer $\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \dots + X + 1$.
  en un autre poly dt l'irréductibilité sera équiv. et auquel on pourra appliquer le critère. Opéra° qu'on peut lui faire subir : addit°, multiplica°, dérivat°, évaluat° en un autre pt
  (conserve pas l'irréd) (divisible)

$$\frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{k-1}$$

- Quels sont les carrés de $\mathbb{Z}/p\mathbb{Z}$. Caractérisa°
  ↳ $x^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si carré} \\ -1 & \text{sinon} \end{cases}$

Commentaires

- Défense :
  * bien d'annoncer la couleur
  * trop de tps pour décrire la partie 2. As dire explicitement avantage des fonc° multiplicatives : il suffit de montrer qu'elles coïncident sr des puissances de p.
  * III. $\Sigma 1/p$ dv est un résultat impt. Historiquement dire que sa utilise la fonc° ζ de Riemann. Un peu plus de trucs culturels à dire
  * IV Donner + d'exemple. + parler des corps finis.

- Plan :

I {
* ordre I : pas vraiment canonique ne marche. On peut remonter le crible d'Eratosthène où est la prop ?

II {
* factorisa° : connaître l'unicité.
* valua° p-adique : pas anecdotique. Sert à dem Tchebytchev (oral)
* Il manque $\Sigma 1/p = \infty$

IV {
* Manque des trucs + gnx sr les corps finis et la réduc° de dpée ?
* Parler de p-gpes et de p-Sylow
* Dvt 2 : il faut savoir que si pas commutatif alors pdt semi-direct et les isomorph. cf savoir et à savoir dem.

* Gnal : on peut permuter des trucs.

- Une leçon où on accepte tt à fait la clar. Ne pas faire un catalogue