Nom:

MARIT

Prénom:

Marcel

Numéro de Jury:

1

Numéros des sujets tirés:

121 / 159

Intitulé du sujet choisi:

Nombres premiers. Applications

I- L'ensemble des nombres premiers

1- Notion de nombres premiers

Théorème 1 : $\mathbb{Z}$ est un anneau euclidien donc factoriel. Ses irréductibles sont 1et-1

Définition 2 (nombre premier) : on appelle nombre premier tout irréductible positif de $\mathbb{Z}$

Remarque 3 : $p \in \mathbb{Z}$ est premier si, et seulement si, il n'admet que deux diviseurs.

Exemple 4 : 2 est l'unique nombre premier pair. 1 n'est pas premier. $561 = 17 \times 11 \times 3$ n'est pas premier

Théorème 5 : L'ensemble des nombres premiers $(\mathcal{P})$ est infini.

Algorithme 6 (Guillod Enthoffer) :

Entrée : $n \geq 2$

Sortie : La liste des nombres premiers inférieurs à n

$P \leftarrow \emptyset$

$L \leftarrow [\![2, n]\!]$

Tant que $L \neq \emptyset$:

| retirer le min de L à L et l'ajouter à P. Retirer tous les multiples de ce min de L

renvoie P

2- Arithmétique et nombres premiers

Théorème 7 : Soit $n \in \mathbb{Z} \setminus \{0\}$. Il existe une unique suite $(\nu_p(n))_{p \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ presque nulle et un unique $\varepsilon \in \{-1, 1\}$ tels que :

$$n = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

$\nu_p(n)$ est appelé valuation p-adique de n

Proposition 8 (pgcd, ppcm) : Soient $n, m \in \mathbb{Z} \setminus \{0\}$ alors :

$$\text{pgcd}(n, m) = \prod_{p \in \mathcal{P}} p^{\min\{\nu_p(n), \nu_p(m)\}}$$

$$\text{ppcm}(n, m) = \prod_{p \in \mathcal{P}} p^{\max\{\nu_p(n), \nu_p(m)\}}$$

Exemple 9 : $\text{pgcd}(561, 66) = 33$

Théorème 10 (Euclide) : Soit $p \in \mathcal{P}$, $(a, b) \in \mathbb{Z}^2$. Si $p | ab$, alors $p | a$ ou $p | b$

Corollaire 11 (Gauss) : Soient $(a, b, c) \in \mathbb{Z}^3$ avec a et b premiers entre eux. Si $a | bc$, alors $a | c$

Application 12 (morphisme de Frobenius) : Soit $p \in \mathcal{P}$ et A un anneau de caractéristique p. L'application $\text{Frob}_p : \begin{cases} A \longrightarrow A \\ x \longmapsto x^p \end{cases}$ est un morphisme d'anneaux.

3- Autour de la répartition des nombres premiers

Définition 13 (fonction de comptage) : On appelle fonction de comptage la fonction $\pi : \mathbb{N} \longrightarrow \mathbb{N}$ telle que $\pi(n)$ est le nombre de nombres premiers inférieurs ou égaux à n.

Exemples 14 :

n	1	2	3	4	5	6	7	8	9
$\pi(n)$	0	1	2	2	3	3	4	4	4

Théorème 15 (des nombres premiers, admis)

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

Corollaire 16 (minoration de Legendre) :

$$\frac{\pi(n)}{n} \xrightarrow[n \to +\infty]{} 0$$

Intercalaire N°

DVT 2

Remarque 17 : On peut comprendre intuitivement ce résultat de la façon suivante : si X_n est une variable aléatoire de loi uniforme sur $[\![1,n]\!]$, alors $\mathbb{P}(X_n \in D) \xrightarrow[n \to +\infty]{} 0$

II- Réduction modulo p

1- Corps $\mathbb{Z}/p\mathbb{Z}$

Théorème 18) : Soit $p \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :
(i) p est premier
(ii) $\mathbb{Z}/p\mathbb{Z}$ est intègre
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un corps

Application 19 : La parabole d'équation $2y = x^2 - 3x + 1$ ne contient pas de point entier.

Application 20 : Soit K un corps fini. La caractéristique de K est nécessairement un nombre premier p, et il existe $\alpha \in \mathbb{N}^*$ tel que $|K| = p^\alpha$

Corollaire 21 (Fermat) : si p est premier, pour tout a premier avec p,
$$a^{p-1} \equiv 1 \ [p]$$

Contre-exemple 22 (Carmichael) : il existe des nombres composé qui satisfont le critère de Fermat. On les appelle nombres de Carmichael. 561 est l'un d'entre eux.

Théorème 23 (nombres de Carmichael) : Soit $n \geq 2$ composé. n est de Carmichael si, et seulement si, pour tout facteur premier p de n, p^2 ne divise pas n et $p-1 \mid n-1$

2- Réduction des polynômes

Proposition 24 : Il existe un unique morphisme d'anneaux
$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$$
envoyant X sur X et coïncidant avec la projection sur $\mathbb{Z}/p\mathbb{Z}$ sur les constantes.

Théorème 25 (Eisenstein) : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ avec $a_n \neq 0$. S'il existe $p \in \mathcal{P}$ tel que $p \nmid a_n$, $p \mid a_k$ pour tout $k < n$ et $p^2 \nmid a_0$, P est irréductible dans $\mathbb{Z}[X]$

Exemple 26 : Si p est premier, $X^n - p$ est irréductible dans $\mathbb{Z}[X]$ quelque soit n.

Lemme 27 : Si p est premier et n est premier avec p, $X^n - 1$ est à racines simples dans $\mathbb{Z}/p\mathbb{Z}[X]$

Application 28 (Dirichlet faible) : pour $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo n.

On aura pour cela besoin de :

Définition 29 (polynôme cyclotomique) : pour $n \in \mathbb{N}^*$, on note μ_n^* l'ensemble des racines primitives n-ièmes de l'unité et
$$\Phi_n := \prod_{\omega \in \mu_n^*} (X - \omega) \in \mathbb{C}[X]$$

3- Résidus quadratiques

Dans toute cette partie, on fixe p un nombre premier impair et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Lemme 30 : L'ensemble $K^\times := \{x^2, x \in \mathbb{F}_p^\times\}$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$. Ses éléments sont les racines de $X^{\frac{p-1}{2}} - 1$.

Application 31 : pour $(a,b,c) \in \mathbb{F}_p^3$, a et b non nuls, l'équation
$$ax^2 + by^2 = c$$
a au moins une solution dans $\mathbb{F}_p$

Définition 32 (symbole de Legendre) : pour $a \in \mathbb{Z}$, on note :
$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ si } p \mid a \\ 1 \text{ si } a \in K^\times \\ -1 \text{ sinon} \end{cases}$$

Proposition 33 : $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p. De plus :
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ [p] \text{ et } \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

DVT 1 (1/2)

Théorème 34 (Réciprocité quadratique) : Soit q un nombre premier impair distinct de p. Alors :
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$ (admis)

Théorème 35 (Lois complémentaires) :
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ si } p \equiv \pm 1 [8] \\ -1 \text{ si } p \equiv \pm 3 [8] \end{cases}$$

Application 36 : Soient q_1 et q_2 deux formes quadratiques non dégénérées sur un $\mathbb{F}_p$-espace vectoriel de dimension finie. On dispose d'un algorithme permettant de tester si elles sont isométriques en réduisant leurs déterminants dans $\mathbb{F}_p^\times$ impasse quelle base modulo $\mathbb{F}_p^{\times 2}$

Définition 37 (symbole de Jacobi) : Soit $n = \prod_{p \in P} p^{\nu_p(n)}$ un entier impair. Pour $a \in \mathbb{Z}$, on pose $\left(\frac{a}{n}\right) := \prod_{p \in P} \left(\frac{a}{p}\right)^{\nu_p(n)}$

Remarque 38 : Si $\left(\frac{a}{n}\right) = -1$, a n'est pas un carré modulo n, mais la réciproque est fausse (par exemple $\left(\frac{-1}{21}\right) = 1$)

Théorème 39 (Solovay-Strassen) : Soit $n > 1$ un entier impair. Les assertions suivantes sont équivalentes :
(i) n est premier
(ii) pour tout a premier avec n, $\left(\frac{a}{n}\right) \equiv (-1)^{\frac{n-1}{2}} [n]$

Algorithme 40 : Entrée : $n, k \in \mathbb{N}$, n impair > 1.
Répéter k fois :
Choisir a au hasard entre 1 et $n-1$
Si $a \wedge n \neq 1$, retourner faux
Si $\left(\frac{a}{n}\right) \not\equiv (-1)^{\frac{n-1}{2}} [n]$ retourner faux.
Retourner vrai.
Si n est premier, l'algorithme renvoie vrai. Sinon, il renvoie faux avec probabilité au moins $1 - \frac{1}{2^k}$

DVT 1 (2/2)

III - p-groupes

On fixe p un nombre premier

Définition 41 (p-groupe) : On appelle p-groupe un groupe fini dont l'ordre est une puissance de p.

Lemme 42 : Le centre d'un p-groupe est non trivial

Corollaire 43 : Soit G un p-groupe d'ordre p^n, $n \geq 2$. Alors G n'est pas simple.

Théorème 44 : Soit G un p-groupe d'ordre p^n. Pour tout $r \leq n$, G admet un sous-groupe d'ordre p^r

Définition 45 (p-Sylow) : Soit G un groupe d'ordre $p^n m$ avec $m \wedge p = 1$. Un p-Sylow de G est un sous-groupe de G d'ordre p^n

Théorème 46 (Sylow) : Si G est un groupe fini et p un diviseur premier de $|G|$, G admet un p-Sylow. De plus, le nombre de p-Sylow de G est congru à 1 modulo p et tous les p-Sylow de G sont conjugués

Application 47 : Un groupe d'ordre 63 n'est pas simple

Application 48 : Soient $p < q$ deux nombres premiers. Alors, si G est un groupe d'ordre pq, on a un produit semi-direct :
$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$$
En particulier, G n'est pas simple.

Intercalaire N°

Annexe : crible d'Eratosthène :

(2)	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	...

(2)	(3)	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	...

(2)	(3)	~~4~~	(5)	~~6~~	7	~~8~~	~~9~~	~~10~~	...