305 : Exercices faisant intervenir les nombres premiers.

Prérequis et notations :

Groupes, p-groupes, série numérique, indicatrice d'Euler, petit théorème de Fermat
$\mathbb{P}$: ensemble des nombres premiers positifs

Exercice 1 : On pose $(p_n)_{n\geqslant 1}$ la suite croissante des nombres premiers et pour $N \in \mathbb{N}^*$, on pose $u_N = \prod_{n=1}^{N} \frac{1}{1-\frac{1}{p_n}}$.

1) Démontrer que pour tout entier naturel M,

$$u_N \geqslant \prod_{n=1}^{N} \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots + \frac{1}{p_n^M}\right)$$

2) En déduire que pour M assez grand on a $u_N \geqslant \sum_{i=1}^{p_N} \frac{1}{i}$, puis conclure que $\sum_{n=1}^{+\infty} \frac{1}{p_n}$ diverge.

3) On note $\pi(n)$ le nombre de nombres premiers inférieurs à n. Montrer que $\pi(n) = o(n)$.

Série divergente, très classique sauf la fin.

On a à peu de frais $\pi(n) = o(n)$! Culture générale $\pi(n) \sim \frac{n}{\ln(n)}$ (théorème des nombres premiers difficile)

Oraux X-Ens Analyse 1 ex. 3.22 p. 166 (dernière édition !)

Exercice 2 : Probabilité que deux entiers soient premiers entre eux

Soit $n \in \mathbb{N}^*$, on pose r_n la probabilité pour que deux entiers choisis aléatoirement dans $[\![1;n]\!]^2$ soient premiers entre eux et on définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et $\mu(p_1 \cdots p_r) = (-1)^r$ si les p_i sont des nombres premiers deux à deux distincts.

1) Montrer que $r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2$, où E désigne la partie entière.

2) Calculer $\sum_{d|n} \mu(d)$

3) Montrer que $\lim_{n\to\infty} r_n = \frac{6}{\pi^2}$

Une utilisation fondamentale des nombres premiers : la décomposition en facteurs premiers.

Utilisation de la formule du crible de Poincaré.

Majoration de l'équivalent de la somme partielle de la série harmonique.

Oraux X-Ens Algèbre 1 ex. 4.33 p. 156

Exercice 3 : Groupe d'ordre pq, centre d'un p-groupe, Th. Cauchy

1) Soit G un groupe abélien d'ordre pq où p et q sont des nombres premiers distincts. Montrer que G est cyclique.
2) Soit G un p-groupe. En considérant l'action de G sur lui même par conjugaison montrer que le centre de G n'est pas trivial. Que dire si $|G| = p^2$?
3) Soit G un groupe fini d'ordre n et p un diviseur premier de n. Montrer que G contient un élément d'ordre p.

Divers résultats sur la théorie des groupes et les nombres premiers.
1) Faux si G non abélien (Contre-exemple : $\mathcal{S}_3$)

Oraux X-Ens Algèbre 1 p. 41-48

3) Gourdon Algèbre p. 27

Exercice 4 : Cryptographie RSA

Soient p et q deux nombres premiers distincts, $n = pq$ et c et d deux entiers tels que $cd \equiv 1 \pmod{\varphi(n)}$, où φ désigne l'indicatrice d'Euler.
Montrer que pour tout $t \in \mathbb{Z}$, $t^{cd} \equiv t \pmod{n}$.

Exemple archi-classique de cryptographie asymétrique. (n, c) est la clef publique et d la clef secrète.
Propriétés de φ, Bézout, Fermat.

Gourdon Algèbre p. 34

Exercice 5 : Lemme de Gauss et Critère d'Eisenstein

1) Soient $P, Q \in \mathbb{Z}[X]$. On note $c(P)$ le contenu de P (le pgcd de ses coefficients). Montrer que $c(PQ) = c(P)c(Q)$.
2) Montrer que si $\Phi \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ alors Φ est irréductible dans $\mathbb{Q}[X]$.
3) On pose $P(X) = a_n X^n + \cdots + a_1 X + a_0$ et on suppose qu'il existe un nombre premier p tel que : $(i) \forall k \in [\![0; n-1]\!], p | a_k \quad (ii) p \nmid a_n \quad (iii) p^2 \nmid a_0$.
Montrer que P est irréductible dans $\mathbb{Q}[X]$.
4) Application : montrer que pour p premier, $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

$\mathbb{Z}/p\mathbb{Z}[X]$ est intègre.

Gourdon Algèbre p. 58

Oraux X-Ens Algèbre p. 189

Cas particulier, polynômes cyclotomiques.

Exercice 6 : Cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$

1) Soit n un nombre entier et φ l'indicatrice d'Euler. Montrer que :

$$n = \sum_{d|n} \varphi(d)$$

2) Montrer que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Dénombrement :
1) Gourdon Algèbre p. 31 (à développer peut être un peu - voir section développement)

Nombre de racines d'un polynôme sur un corps.
2) Perrin, Cours d'algèbre p. 74

Exercice 7 : Wilson et infinité nombres premiers congrus à 1 mod 4

1) Montrer qu'un entier $p \geqslant 2$ est premier ***ssi*** $(p-1)! \equiv -1 \pmod{p}$.
2) Soit $p > 2$ un nombre premier. Montrer que $-\bar{1}$ est un carré dans dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod{4}$.
3) En déduire qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod{4}$.

$\mathbb{Z}/p\mathbb{Z}$ est un corps.
1) Gourdon algèbre p. 9

2) 3) Gourdon Algèbre p. 37

D'autres pistes :

a) **La méthode de factorisation ρ de Pollard**
Assez jolie, elle peut tout à fait faire l'objet d'une démonstration avec l'algorithme de Brent (ou Floyd) et de l'utilisation de l'outil informatique le jour de l'oral (un programme en Python par exemple - voir la section algorithme de ce site).
Références :
"Cours d'algèbre" de Michel Demazure (CASSINI)
"Algorithmique Algébrique" de P. Naudin et C. Quitté (MASSON)
"The art of computer programming : fundamental algorithms" de Donald Knuth (Addison-Wesley)

b) **Test de primalité de Rabin-Miller**
Là encore l'outil informatique est indispensable pour une prestation à l'oral.
Références :
"Cours d'algèbre" de Michel Demazure (CASSINI)
"Prime numbers, a computational perspective" de R. Crandall et C. Pomerance (SPRINGER)

c) **Théorème de Sophie Germain**
Un peu plus théorique, ce cas particulier du grand théorème de Fermat peut faire aussi un beau développement.
Référence :
"Oraux X-Ens, Algébre 1" de S. Francinou, H. Gianella et S. Nicolas (CASSINI)

Remarque : évidemment il faut faire des choix...