A réviser : Groupes cycliques, ordre, sous groupe, morphismes, Théorème de Lagrange, indicatrice d'euler, morphismes d'anneaux, groupe $\mathbb{U}$,Tout élément non nul de $\mathbb{K}_n[X]$ admet au plus n racine.

Partie du programme abordée en plus : Codage et cryptage. Algorithmique. Primalité. Application de $\mathbb{Z}[i]$.

Exercice I(sous groupes cycliques)
1) Montrer que tout sous groupe d'un groupe cyclique est cyclique.
2) Soient d, n des entiers naturels non nuls tels que d divise n. Montrer qu'il existe un unique sous groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ (on pourra préalablement déterminer le groupe G_d des éléments dont l'ordre divise d.)
3)En déduire que $n = \sum_{d|n} \varphi(d)$.

Dans la suite K désigne un corps fini commutatif et K^* le groupe des inversible de K.On pose $n = |K^*|$
4)a) soit d un diviseur de n. Montrer que le groupe engendré par l'ensemble A_d des éléments d'ordre d est vide ou isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et déduire que $|A_d| = \varphi(d)$ ou 0.
b) En déduire que K^* est cyclique (on pourra se servir du 3)).

Exercice II (test de primalité de lucas-lehmer)
1) Montrer qu'un entier $p \geq 2$ est premier si et seulement si $(\mathbb{Z}/p\mathbb{Z}^\times, \times)$ est de cardinal $p-1$.
2) Montrer qu'un entier $p \geq 2$ est premier si et seulement si $(\mathbb{Z}/p\mathbb{Z}^\times, \times)$ admet un élément d'ordre $p-1$. (on pourra utiliser l'exo précédent)
3) On considère ici $p = 2^{32}3^{32}5^{32} + 1$ et $n = p - 1$ on suppose qu'on a vérifié que $2^n \equiv 1[n]$ et que 2 élévé aux puissances $\frac{n}{2}, \frac{n}{3}$ et $\frac{n}{5}$ n'est pas congru à $1[n]$. Prouver alors que p est premier.

Exercice III (Logarithme discret et echange de clé de Diffie-Hellman)
Soit G un groupe, $g \in G$ d'ordre n et $a \in [1, .., n]$.
1) "Calcul de puissance" : On suppose que a s'ecrit $a_k a_{k-1} ... a_1$ en base 2. Montrer qu'on peut, connaissant g et a, calculer g^a en moins de $2\log_2(n)$ multiplications.
2) "détermination de a" : On suppose connus g et g^a mais pas a.
Pour retrouver a on ne sais que calculer $g, g^2 = g \times g, g^3 = g^2 \times g, ...$ jusqu'à tomber sur g^a . On note t_a le nombre d'opérations nécessaires pour determiner a de la sorte.
Calculer le nombre moyen d'opération $\frac{\sum_{a\in[1,..,n]} t_a}{n}$.
3) Protocole de Diffie Hellman : Alice et bob veulent choisir une clé commune

pour des communications futures. Alice choisit un groupe G , $g \in G$ et $a \in \mathbb{Z}$ et transmet G, g et g^a à Bob.
Bob choisit $b \in \mathbb{Z}$ calcule $g^{ab} = (g^a)^b$ et transmet alors g^b à Alice qui peut a son tour calculer g^{ab}.
g^{ab} qui n'a pas transité par le réseau peut alors leur servir de clé.
Expliquez pourquoi ce protocole fonctionne.

Exercice IV (le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z}^\times, \times)$ est cyclique)
Soit $p \geq 3$ un nombre premier et α un entier ≥ 2.
1)a) Montrer par récurrence que $\forall k \in \mathbb{N}^* \lambda \in \mathbb{N}^*$ tel que $\lambda \wedge p = 1$ et $(1+p)^{p^k} = 1 + \lambda p^{k+1}$
b) En déduire que $(1+p)$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z}^\times, \times)$
2)a) Montrer qu'il y a un morphisme d'anneaux naturel de $(\mathbb{Z}/p^\alpha\mathbb{Z}, +, \times)$ dans $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ et que ce dernier se restreint en un morphisme de groupes surjectif de $(\mathbb{Z}/p^\alpha\mathbb{Z}^\times, \times)$ dans $(\mathbb{Z}/p\mathbb{Z}^*, \times)$.
b) En déduire qu'il existe dans $(\mathbb{Z}/p^\alpha\mathbb{Z}^\times, \times)$ un élément d'ordre $p-1$, puis que $(\mathbb{Z}/p^\alpha\mathbb{Z}^\times, \times)$ est cyclique.

Exercice V (Sous-groupes de $(\mathbb{U}, \times)$)
Montrer qu'un sous-groupe du groupe $\mathbb{U}$ des complexes de module 1 est soit fini et alors égal à un $\mathbb{U}_n$ où n est son ordre, soit partout dense dans $\mathbb{U}$.
(dans le cas d'un sous groupe infini utiliser la compacité de $[0, 2\pi]$ et majorer la distance entre e^{ia} et e^{ib} en fonction de $a - b$).

EXO VI (Somme de deux carrés) L'exercice qui suit étudie l'ensemble Σ des entiers naturels s'écrivant comme somme de deux carrés (pour approfondir voir le "cours d'algèbre" de Perrin).
On considère l'anneau $\mathbb{Z}[i]$ des entiers de gauss. On rapelle que $\mathbb{Z}[i]$ est l'ensemble des nombres compexes dont la partie réelle et la partie imaginaire sont des entiers relatifs.
A tout élément z de $\mathbb{Z}[i]$ on associe sa norme arithmétique $N(z)$ définie par $N(z) = z\overline{z}$.
1)Montrer que 0,1 et tous les carrés d'entiers sont des éléments de Σ.
2)Montrer que Σ est l'ensemble des normes arithmétiques des éléments de $\mathbb{Z}[i]$.
3)En déduire que Σ est stable par multiplication.
4)Montrer que les inversible de $\mathbb{Z}[i]$ sont les éléments de norme arithmétique égale à 1.
5)Soit $p \in \mathbb{N}$ un nombre premier , montrer que si $p \equiv 3[4]$ on a $p \notin \Sigma$.
6)Soit $p \in \mathbb{N}$ un nombre premier, montrer que

$$p \in \sum \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$

.