Sorbonne Université
Année universitaire 2023-2024, Master 1, *Théorie des nombres I* (UE 4MA033).
Examen partiel, le 14 février 2024.
Durée : 2h00. Les appareils électroniques et documents sont interdits.

Exercice 1.

(a) Donnez un générateur de $(\mathbb{Z}/11\mathbb{Z})^\times$.

(b) Décrire explicitement un caractère d'ordre 10 de $(\mathbb{Z}/11\mathbb{Z})^\times$, en donnant la liste de ses valeurs sur tous les éléments de ce groupe.

Exercice 2. Soit G un groupe abélien fini. Soit θ l'application de G vers l'ensemble des applications de $\widehat{G}$ vers $\mathbb{C}^\times$ qui envoie un élément g sur $f \mapsto f(g)$.

(a) Montrez que pour tout $g \in G$ l'application $\theta(g) \colon \widehat{G} \to \mathbb{C}^\times$ appartient au groupe $\widehat{\widehat{G}}$ des caractères de $\widehat{G}$.

(b) Montrez que θ est un morphisme de groupes de G vers $\widehat{\widehat{G}}$.

(c) Montrez que θ est un isomorphisme.

Exercice 3.

(a) Calculez 100, puis 1000, puis 2000 modulo 23 ; on donnera à chaque fois la valeur sous forme d'un entier compris entre (-11) et 11.

(b) Soient a et b deux entiers supérieurs ou égaux à 2. Montrez que $2^{ab} - 1$ n'est pas premier.

(c) Déduire de ce qui précède une condition nécessaire sur un entier n pour que $2^n - 1$ soit premier.

(d) Montrez par un contre-exemple que cette condition nécessaire n'est pas suffisante. *Indication : il faut être un peu patient car les premières valeurs qu'on teste ne donnent pas de contre-exemple. Le petit calcul de la question (a) pourra servir.*

Exercice 4.

(a) Si a est un entier impair au moins égal à 3 et b un entier au moins égal à 1, montrez que $2^{ab} + 1$ n'est pas premier.

(b) En déduire que si $2^m + 1$ est premier alors m est une puissance de 2. On se propose dans ce qui suit de s'intéresser à la réciproque. Pour tout $n \geqslant 0$ on pose $F_n = 2^{2^n} + 1$.

(c) Soit n un entier et soit p un diviseur premier de F_n. Quel est l'ordre (multiplicatif) de 2 modulo p ? En déduire que p est de la forme $k \cdot 2^{n+1} + 1$ pour un certain entier k.

(d) Vérifiez que F_0, F_1, F_2 et F_3 sont premiers.

(e) On se propose de montrer que $F_4 = 2^{16} + 1 = (256)^2 + 1 = 65537$ est premier.

- (e1) Montrez qu'il suffit pour ce faire de prouver que pour tout nombre premier p de la forme $32k+1$ avec $1 \leqslant k \leqslant 7$, l'entier p n'est pas diviseur de F_4.
- (e2) Vérifiez que l'ensemble des nombres premiers de la forme $32k+1$ avec $1 \leqslant k \leqslant 7$ est $\{97, 193\}$.
- (e3) Montrez que ni 97 ni 193 ne divisent F_4 (utilisez l'égalité $F_4 = 2^{16}+1$ plutôt que la valeur explicite de F_4), et conclure.

(f) On se propose de montrer que $F_5 = 2^{32}+1$ n'est pas premier. En remarquant que $641 = 640+1 = 625+16$, montrez que F_5 est divisible par 641 et conclure.

Remarque : on peut vérifier (mais on ne demande pas de le faire) que 641 *est premier, et est le plus petit diviseur premier de F_5. On ne connaît à ce jour aucun $n \geqslant 5$ pour lequel F_n soit premier.*

Exercice 5. On se propose de déterminer de deux façons différentes l'ensemble des nombres premiers p tels que $(\mathbb{Z}/p\mathbb{Z})^\times$ contienne une racine cubique primitive de l'unité (c'est–à-dire un élément d'ordre 3).

(a) *Première méthode : par la théorie des groupes cycliques.*

- (a1) Soit G un groupe cyclique. À quelle condition sur $|G|$ le groupe G possède-t-il un élément d'ordre 3 ?
- (a2) Soit p un nombre premier. À l'aide de la question précédente, donnez une condition nécessaire et suffisante sur p pour que $(\mathbb{Z}/p\mathbb{Z})^\times$ possède un élément d'ordre 3.

(b) *Seconde méthode : par les équations quadratiques.*

- (b1) Soit p un nombre premier *impair* et soient a et b deux éléments de $(\mathbb{Z}/p\mathbb{Z})$. Montrez que X^2+aX+b a une racine dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si a^2-4b est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et si c'est le cas, décrire toutes les racines de X^2+aX+b dans $\mathbb{Z}/p\mathbb{Z}$.

  Montrez par un contre-exemple explicite que cette équivalence est fausse lorsque $p=2$.
- (b2) Soit p un nombre premier différent de 3. Montrez que $(\mathbb{Z}/p\mathbb{Z})^\times$ possède une racine cubique primitive de l'unité si et seulement si X^2+X+1 possède une racine dans $\mathbb{Z}/p\mathbb{Z}$.
- (b3) Utilisez ce qui précède pour retrouver le résultat établi en (a2).