ARITHMETIQUE ET THEORIE DES GROUPES, II

Rappels théoriques :
Voici quelques mots clés qui doivent guider vos révisions :

a) groupe, sous-groupe, morphismes de groupes, classe latérale modulo un sous-groupe, théorème de Lagrange, sous-groupe normal (= distingué), groupe quotient, théorèmes d'isomorphismes, groupe cyclique, petit théorème de Fermat, critère de divisibilité.
b) Congruences sur $\mathbb{Z}$ et théorème chinois, fonction d'Euler et éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, éléments premiers et irréductibles, anneaux factoriels principaux, euclidiens, équations diopharitiennes, rationnalité et irrationnalité, théorème de Bezout, pgcd et ppcm,

EXERCICES SUPPLEMENTAIRES

(1) Soit $(a, b, c) \in \mathbb{Z}^3$
   a) Montrer qu'il existe $(x, y) \in \mathbb{Z}^2$ tel que $ax + by = c$ ssi le pgcd de a et b divise c
   b) "Trouver" toutes les solutions entières de 1).
   c) Trouver le plus petit entier positif congru à 1 modulo 1000 et à 8 modulo 761
   d) Trouver toutes les solutions entières de $1027\ x + 712\ y = 1$
(2) Calculer le reste de $(37)^{13}$ divisé par 17
(3) "Trouver" les triplets $(a, b, c) \in \mathbb{Z}^3$ tan $a^2 + b^2 = c^2$ (aide : Montrer que les solutions peuvent s'écrire sous la forme

$$\begin{cases} a = k(u^2 - v^2) \\ c = k(u^2 + v^2) \\ a = 2uv \end{cases}$$

où $k \in \mathbb{Z}$, $(u, v) \in \mathbb{Z}^2$ et pgcd $(u, v) = 1$)
(4) a) La congruence $ax \equiv a$ (mod n) est résoluble (en x ssi pgcd (a, n) divise b
   b) Si le système $x \equiv b$ (mod m) et $x \equiv b$ (mod n) est résoluble alors $a \equiv b$ (mod pgcd (m, n))
5) Montrer que pour $d\{-2, -1, 2, 3\}$ $\mathbb{Z}\left[\sqrt{d}\right]$ est euclidien.
(5) Déterminer tous les couples de groupes isomorphes parmi
   $A = \frac{\mathbb{Z}}{14\mathbb{Z}} \oplus \frac{\mathbb{Z}}{12\mathbb{Z}} \oplus \frac{\mathbb{Z}}{72\mathbb{Z}}$; $B = \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{28\mathbb{Z}} \oplus \frac{\mathbb{Z}}{72\mathbb{Z}}$; $C = \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{36\mathbb{Z}} \oplus \frac{\mathbb{Z}}{56\mathbb{Z}}$.
(6) Soit G un groupe et soient H et K deux sous-groupes de G. Montrer que, si H est distingué dans G, alors l'ensemble des produits hk, où $h \in H$ et $k \in K$, est un sous-groupe de G.
(7) Notons ϕ l'indicatrice d'Euler. Soit G un groupe d'ordre n qui contient au plus $\phi(d)$ éléments d'ordre d pour tout diviseur d de n tel que $d < n$. Montrer que G est cyclique.
(8) Calculer le *reste* r de la division euclidienne de a par b dans les cas suivants:
   (a) $a = 1234565789012345 \quad b = 11$
   (b) $a = 2000^{2000} \quad b = 7$
   (c) $a = 53^{101} \quad b = 101$
   (d) $a = 5^{512} \quad b = 1024$
   (e) $a = 24^{24} \quad b = 23^2$
   (f) $a = 3^{(5^9)} \quad b = 17$
(9) Résoudre les équations $x^4 = 1$ et $x^3 = 11$ dans $\frac{\mathbb{Z}}{53\mathbb{Z}}$.
(10) On considère le nombre $M = 13^{13} - 1 = 3028751065992252$.
   (a) Montrer, sans calculs explicites, que M est divisible par $12 = 13 - 1$.
   (b) Montrer qu'un diviseur premier de M qui ne divise pas 12 est congru à 1 modulo 26.

(c) Utiliser les points précédents (et la table des indices) pour déterminer tous les diviseurs premiers inférieurs à 100 de M.

(11) (a) Décomposer le nombre $\alpha = -2 + 16i$ en un produit d'éléments premiers dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

(b) Soit p un nombre premier congru à 3 modulo 4. Montrer que les seules solutions $(x, y) \in \mathbb{Z}^2$ de l'équation

$$x^2 + y^2 = p^2$$

sont $(\pm p, 0)$ et $(0, \pm p)$. Indication : Si (x, y) est une solution, on pourra considérer la décomposition en facteurs premiers de l'entier de Gauss $x + iy$.