UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n° 1 : Primalité, Corps finis

Primalité et $(\mathbb{Z}/n\mathbb{Z})^\times$

Tests de compréhension

Test 1.

a. Rappeler pourquoi si K est un corps, tout polynome de degré n a coefficients dans K a au plus n racines.

b. Montrer que l'énoncé est toujours vrai si on remplace K par un anneau intègre.

c. Donner un contre-exemple dans un anneau $\mathbb{Z}/k\mathbb{Z}$.

Test 2.

Soit $n = 2^4 \cdot 3^5 \cdot 5^6 \cdot 7 = 425250000$.

a. Calculer la valeur de l'indicatrice d'Euler $\phi(n)$.

b. Calculer le pgcd des ordres des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.

On trouve $\phi(n) = 97200000$. Le ppcm des ordres est vaut 1012500.

Exercices

Exercice 3. Nombres premiers congrus à -1 modulo 4

Il s'agit de montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 4. Supposons le contraire, et soient $p_1, \ldots, p_k$ la liste complète de ces nombres premiers.

a. Soit $n = 4p_1 \ldots p_k - 1$. Que vaut n modulo 4 ?

b. Montrer que tout facteur premier de n est égal à 1 modulo 4.

c. Déduire une contradiction.

d. Montrer de la même façon qu'il y a une infinité de nombres premiers congrus à -1 modulo 6.

Exercice 4. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique pour p premier impair

a. Quel est le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$?

b. Soit U le sous-groupe des éléments de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ congrus à 1 mod p. Quel est son cardinal ?

c. Montrer par récurrence que pour $n \geq 1$, $(1+pa)^{p^n} = 1 + p^{n+1}a \pmod{p^{n+2}}$.

d. Montrer que si $x \in \mathbb{Z}$ vérifie $x = 1 \pmod{p}$ et $x \neq 1 \pmod{p^2}$, alors x est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En déduire que U est cyclique.

e. En utilisant que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ possède un élément y dont l'ordre est un multiple de $p-1$.

f. Conclure que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

g. Où utilise-t-on que $p \neq 2$?

Exercice 5. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique, mais presque.

Soit $\alpha \geq 3$.

a. Décrire les groupes $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ et $(\mathbb{Z}/8\mathbb{Z})^\times$. Sont-ils cycliques ?

b. Montrer par récurrence que $(1+4a)^{2^n} = 1 + 2^{n+2}a \mod 2^{n+3}$.

c. Montrer que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Donner au groupe cyclique $U' = \langle 5 \rangle$ une description analogue a celle de U dans l'exercice précédent.

d. Conclure que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est le produit direct $\{\pm 1\} \times U'$.

Exercice 6. Pour quelles valeurs de n le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

a. Soient G, H deux groupes cycliques d'ordres n, m. Montrer que $G \times H$ est cyclique si et seulement si n et m sont premiers entre eux.

b. Pour quelles valeurs de n le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ? (utiliser les deux exercices précédents)

Exercice 7. Nombres de Carmichael

Rappelons que n est un nombre de Carmichael si n n'est pas premier, et si $a^{n-1} = 1 \pmod{n}$ pour tout a premier avec n.

a. Soit n un nombre sans facteur carré, tel que pour tout diviseur premier p de n, $p-1$ divise $n-1$. Montrer que n est de Carmichael ou premier.

b. Montrer que 561 est de Carmichael.

c. On suppose qu'il existe un nombre premier p tel que $p^2 \mid n$. Montrer que l'élément $a = 1 + \frac{n}{p}$ est d'ordre p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

d. En déduire qu'un nombre de Carmichael est toujours sans facteur carré.

e. Montrer qu'un entier $n > 1$ non premier, sans facteur carré est un nombre de Carmichael si et seulement si pour tout facteur premier p de n, on a $(p-1) \mid (n-1)$.

f. Montrer que n non premier est un nombre de Carmichael si et seulement si $a^n = a \pmod{n}$ pour tout $a \in \mathbb{Z}$.

Exercice 8. Nombres de Fermat.

On note $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Fermat a vu que $F_0, F_1, \ldots, F_4$ étaient premiers et a conjecturé que c'était le cas pour tout n. Euler a réalisé que F_5 n'était pas premier, et on ne connaît pas d'autre n tq F_n soit premier.

a. Montrer que si $2^k + 1$ est premier, alors k est une puissance de 2.

b. En exhibant une relation de Bezout, montrer que si $n \neq m$, F_n et F_m sont premiers entre eux.

c. Soit p un nombre premier divisant F_n. Montrer que 2 est d'ordre 2^{n+1} dans $(\mathbb{Z}/p\mathbb{Z})^\times$. En déduire que $p = 1 \mod 2^{n+1}$.

d. En supposant $n \geq 2$ (...), et en admettant que 2 est un carré modulo p (cf lois de réciprocités quadratiques), montrer que $p = 1 \mod 2^{n+2}$.

e. Au vu de la question d., combien de candidats y a-t-il pour des diviseurs premiers de F_4 ? de F_5 ? A l'aide d'un ordinateur ou d'une calculatrice, trouver un diviseur premier de F_5.

Extensions de corps

Tests de compréhension

Test 9.

Soit A un anneau fini. On suppose que A est intègre. Montrer que c'est un corps. (Indication : pour $a \neq 0$, considérer l'application $\mu_a : x \mapsto ax$).

Test 10.

a. Un corps fini peut-il être algébriquement clos ?

b. Montrer que tout morphisme de corps est injectif.

c. Soit P un polynome dans $K[X]$. Montrer que $K[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercices

Exercice 11. Racines multiples, et dérivée

Soit K un corps, et $P \in K[X]$ un polynome ayant une racine α dans une extension E de K.

a. Montrer que α est une racine multiple de P si et seulement si $P'(\alpha) = 0$.

b. Montrer que si P est irréductible et que α est une racine multiple de P alors $P' = 0$.

c. Montrer que $P' = 0$ si et seulement si K est de caractéristique positive p, et que $P(X) = Q(X^p)$ pour un certain polynome Q.

d. Supposons en outre que le morphisme de Frobenius $\phi : K \to K$ est surjectif, par exemple un si K est un corps fini (on dit que K est un corps *parfait*).
Montrer que tout polynôme de la forme $P(X) = Q(X^p)$ s'écrit $P(X) = R(X)^p$ pour un certain polynôme $R \in K[X]$.

e. En deduire qu'un polynôme irréductible à coefficients dans un corps parfait n'a de racine multiple dans aucune extension.

f. Que se passe-t-il pour $K = \mathbb{Z}/p\mathbb{Z}(t)$, avec le polynôme $P(X) = X^p - t$?
On pourra démontrer qu'il est irréductible en utilisant le fait que $P' = 0$, et en montrant montrer que s'il a un facteur irréductible A non trivial, alors $A^i | P$ pour $i = 2, \ldots, p$, et en déduire une contradiction.

Exercice 12.

Soit K un corps, et soit $P \in K[X]$ un polynôme irréductible sur K.

1. Soit K' un corps de rupture de P sur K, et soit L une extension de K. Montrer qu'il y a une bijection naturelle entre les morphismes K-linéaires de corps de K' dans L et les racines de P dans L.
2. On suppose que le corps K est de caractéristique 0. Combien y a-t-il de morphismes K-linéaires de corps de K' dans une clôture algébrique $\overline{K}$ de K ?

Exercice 13.

On considère la suite d'entiers définie par

(i) $u_0 = 3$, $u_1 = 0$, $u_2 = 2$;

(ii) $u_{n+3} = u_n + u_{n+1}$ pour $n \geqslant 0$.

Montrer que si p est un nombre premier, alors u_p est multiple de p. (On pourra se placer dans un corps de décomposition de $X^3 - X - 1$ sur $\mathbb{F}_p$, et montrer que $u_n = \alpha^n + \beta^n + \gamma^n$, où α, β, γ sont les racines de $X^3 - X - 1$).

Notez que, comme pour le petit théorème de Fermat, la réciproque est fausse.

Corps finis

Test de compréhension

Test 14.

Écrire la table de multiplication de $\mathbb{F}_4$.

Test 15.

Soit p un nombre premier, et K un corps de cardinal $q = p^r$. Quelle est la structure de groupe additif de K ?

Exercices

Exercice 16.

Soit p un nombre premier, et K une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$. Quelles sont les racines p-ièmes de l'unité ? Et les racines p^k-ièmes ?

Soit $n = p^\alpha m$ avec $m \wedge p = 1$. Combien y a-t-il de racines n-ièmes de l'unité dans K ?

Exercice 17.

Soit $P = X^3 + 2X + 1 \in \mathbb{F}_3[X]$. Posons $\mathbb{L} = \mathbb{F}_3[X]/(P)$ et α la classe de X dans $\mathbb{L}$.

1. Montrer que P est irréductible sur $\mathbb{F}_3$. En déduire que $\mathbb{L}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? Donner une base du $\mathbb{F}_3$-espace vectoriel $\mathbb{L}$.
2. Quels sont les ordres possibles pour les éléments de $\mathbb{L}^\times \setminus \mathbb{F}_3^\times$ (dans le groupe $\mathbb{L}^\times$).
3. L'objet de la question est de montrer que α est un générateur de $\mathbb{L}^\times$.
   (a) Montrer que $\alpha^{13} = -1$ si et seulement si P divise $(X-1)^4X + 1$ dans $\mathbb{F}_3[X]$.
   (b) Conclure.
4. Le polynôme $Q = X^4 + X^3 + X^2 + X + 1$ a-t-il une racine dans $\mathbb{L}$?

Exercice 18.

Soit $P = X^3 + X + 1$ dans $\mathbb{F}_5[X]$ et l'anneau $K = \mathbb{F}_5[X]/(P)$. On note α la classe de X.

1. Montrer que K est un corps. Donner sa caractéristique, son cardinal ainsi qu'une base $\mathcal{B}$ de K en tant que $\mathbb{F}_5$-espace vectoriel.
2. Donner les développements de α^3, α^{15} et α^{30} dans $\mathcal{B}$. Donner l'ordre de α et de 2α dans $K^\times$.
3. Déterminer les coordonnées de l'inverse de $1 + \alpha$ dans $\mathcal{B}$.
4. Que vaut $P(\alpha^5)$? Donner les racines de P dans K.

Exercice 19.

Soit $P = X^2 + X + 2 \in \mathbb{F}_5[X]$. On note $\mathbb{K} = \mathbb{F}_5[X]/(P)$ et α la classe de X dans $\mathbb{K}$.

1. Montrer que P est irréductible sur $\mathbb{F}_5$. En déduire que $\mathbb{K}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? En donner une base comme $\mathbb{F}_5$-espace vectoriel.
2. Exprimer toutes les puissances distinctes de α dans cette base. Quel est l'ordre de α dans $\mathbb{K}^\times$?
3. Montrer que $\mathbb{F}_5 = \left\{x \in \mathbb{K} / x = x^5\right\}$.
4. Soit $a \in \mathbb{K} \setminus \mathbb{F}_5$. Montrer que le polynôme $P_a = (X-a)(X-a^5)$ est irréductible dans $\mathbb{F}_5[X]$.
5. Montrer que si $Q \in \mathbb{F}_5[X]$ alors a est racine de Q si et seulement si P_a divise Q.
6. Factoriser le polynôme $X^{25} - X$ dans $\mathbb{F}_5[X]$ et donner les racines dans $\mathbb{K}$ de chaque facteur.

Exercice 20.

Quels sont les sous-corps de $\mathbb{F}_{64}$?

Exercice 21.

Trouver un générateur de $\mathbb{F}_{31}^\times$.

Exercice 22.

1. Déterminer tous les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$.
2. Soit $f = 2X^5 + X^4 + 2X^3 + X + 2$.
   (a) Donner la classe $\bar{f}$ de f dans l'anneau $\frac{\mathbb{F}_3[X]}{(2X^2+2)}$.
   (b) Donner la classe $\widetilde{f}$ de f dans l'anneau $\frac{\mathbb{F}_3[X]}{(2X^2+X+1)}$.
   (c) f a-t-il des racines dans $\mathbb{F}_3$?
   (d) f est-il irréductible dans $\mathbb{F}_3[X]$?
3. On considère l'anneau $A = \frac{\mathbb{F}_3[X]}{(f)}$. Soit $f_1 = 2X^2 + X + 1$.
   (a) Montrer que A est isomorphe à un anneau produit $\frac{\mathbb{F}_3[X]}{(f_1)} \times \frac{\mathbb{F}_3[X]}{(f_2)}$. On précisera le polynôme f_2 et l'isomorphisme mis en jeu. Indication : lemme chinois.
   (b) A est-il un corps ? A est-il un anneau intègre ?
4. Soient $A_1 = \frac{\mathbb{F}_3[X]}{(f_1)}$ et $A_2 = \frac{\mathbb{F}_3[X]}{(f_2)}$. Soit ω une racine de f_2 dans A_2.
   (a) A_1, A_2 sont-ils des corps ?
   (b) ω est-il un générateur du groupe multiplicatif $A_2^\times$?
   (c) Donner le polynôme minimal de ω^2 sur $\mathbb{F}_3$.

Exercice 23.

Décomposer le polynôme $X^4 + 1$ en produit de facteurs irréductibles dans $\mathbb{F}_7[X]$.

Exercice 24.

Montrer qu'il n'y a pas d'entier impair $n > 1$ tel que $a^{n-1} \equiv -1 \pmod{n}$ pour un certain $a \in \mathbb{Z}$.

Témoins de Miller-Rabin

Exercice 25. Densité des témoins de Miller-Rabin

On se propose de montrer que pour tout nombre n impair qui n'est pas premier, au moins la moitié des éléments de $\{1, \dots n-1\}$ sont des témoins de Miller-Rabin. En se fatigant un peu plus, on peut montrer que cette proportion est en fait au moins égale à 3/4.

On sait que si n n'est pas un nombre de Carmichael, au moins la moitié des éléments de $\{1, \dots, n-1\}$ sont des témoins de Fermat. Puisque les témoins de Fermat sont en particulier des témoins de Miller-Rabin, on peut donc supposer que n est un nombre de Carmichael, ce qu'on fait dans toute la suite. Rappelons que ceci implique que n est sans facteur carré (Cf exercice 7).

Ecrivons $n - 1 = 2^s m$ avec m impair. Soit $\varepsilon_i : \mathbb{Z}/n\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times$ défini par $\varepsilon_i(x) = x^{2^i m}$, et soit $K_i = \ker \varepsilon_i$.

a. Montrer que si $x \in \{1, \dots n-1\}$ a un facteur commun avec n, c'est un témoin de Fermat (donc de Miller-Rabin). En déduire qu'il suffit de montrer que parmi les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$, au moins la moitié sont des témoins de Miller-Rabin.

b. Montrer que $K_0 \subset K_1 \subset \cdots \subset K_s$, et que $K_s = (\mathbb{Z}/n\mathbb{Z})^\times$.

c. Montrer que $K_0 \neq (\mathbb{Z}/n\mathbb{Z})^\times$ (trouver un élément qui n'est pas dans K_0).

Soit $i < s$ le plus grand entier tq $K_i \neq (\mathbb{Z}/n\mathbb{Z})^\times$.

d. Supposons d'abord que l'image de ε_i n'est pas contenue dans $\{-1, 1\}$. En déduire qu'au moins la moitié des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont des témoins de Miller-Rabin.

On cherche donc à montrer que l'image de ε_i n'est pas contenue dans $\{-1, 1\}$.

e. Montrer l'existence d'un facteur premier p de n et de $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\varepsilon_i(b) \neq 1 \pmod{p}$.

f. Soit $q \neq p$ un autre facteur premier de n. Montrer l'existence de $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\varepsilon_i(c) = \varepsilon_i(b) \mod p$ et $\varepsilon_i(c) = 1 \mod q$.

g. Déduire que $\varepsilon_i(c) \neq \pm 1$ et conclure.