UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°2 : Corps finis 2

Exercice 1

On dira qu'un entier impair n est pseudopremier pour un entier a compris entre 1 et $n-1$ si a est premier à n et $a^{n-1} = 1 \pmod{n}$.

1. Trouver tous les entiers a pour lesquels 15 est un nombre pseudopremier.
2. Pour quelles valeurs de a entre 1 et 90 le nombre 91 est-il pseudopremier ?
3. Montrer que si p et $2p-1$ sont premiers, alors $n = p(2p-1)$ est pseudopremier pour à peu près la moitié des nombres a possibles dans $\{1, \dots, n\}$, plus précisément pour ceux qui sont premiers à n et qui sont des carrés dans $\mathbb{F}_{2p-1}$.
4. On pose $n = 561$. Calculer $\varphi(n)$. Pour quelles valeurs de a entre 1 et 561 le nombre n est-il pseudopremier ?

Exercice 2

Un entier n est appelé nombre de Carmichael si, pour tout entier a entre 1 et $n-1$ premier avec n, on a $a^{n-1} = 1 \pmod{n}$.

1. Soit $N > 1$ un entier. On suppose qu'il existe un nombre premier p tel que $p^2 \mid N$. Posons $a = 1 + \frac{N}{p}$. Montrer que a est d'ordre p dans $(\mathbb{Z}/N\mathbb{Z})^\times$.
2. En déduire qu'un nombre de Carmichael est toujours sans facteur carré.
3. Montrer qu'un entier $n > 1$ sans facteur carré est un nombre de Carmichael si et seulement si pour tous les nombre premiers p divisant n on a $(p-1) \mid (n-1)$.

Exercice 3

1. Trouver tous les nombres de Carmichael de la forme $3pq$ avec p et q premiers.
2. Trouver tous les nombres de Carmichael de la forme $5pq$ avec p et q premiers.
3. Montrer que pour tout nombre premier r, il existe un nombre fini de nombres de Carmichael de la forme rpq avec p et q premiers.

Exercice 4

1. Montrer que les nombres 1105 $(5 \times 13 \times 17)$, 1729 $(7 \times 13 \times 19)$ et 2465 $(5 \times 17 \times 29)$ sont des nombres de Carmichael.

2. Soit n un entier tel que $6n + 1$, $12n + 1$ et $18n + 1$ sont premiers. Montrer que $m = (6n + 1)(12n + 1)(18n + 1)$ est un nombre de Carmichael.

Exercice 5

Soient $b > 1$ et p un nombre premier impair ne divisant pas b, $b-1$ ou $b+1$. Soit $n = \frac{b^{2p}-1}{b^2-1}$.

1. Montrer que $\frac{b^p-1}{b-1}$ est un entier non inversible qui divise n. En déduire que n n'est pas premier.
2. Montrer que $n - 1$ est pair, puis que que $2p$ divise $n - 1$.
3. Montrer que n est pseudopremier pour b.
4. En déduire que pour tout entier b, il y a une infinité de nombres pseudopremiers pour b.

Exercice 6

1. Montrer que $\left(\frac{2m}{n}\right) = \left(\frac{m}{n}\right)$ si $n \equiv \pm 1 \pmod 8$ et $\left(\frac{2m}{n}\right) = -\left(\frac{m}{n}\right)$ sinon.
2. Vérifier que si m et n sont tous les deux impairs, alors $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ sauf si m et n sont tous les deux congrus à 3 modulo 4, auquel cas $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Exercice 7

1. Calculer les symboles de Legendre $\left(\frac{16}{229}\right)$, $\left(\frac{19}{229}\right)$, $\left(\frac{2}{229}\right)$, $\left(\frac{38}{229}\right)$.
2. Calculer le symbole de Legendre $\left(\frac{365}{1847}\right)$ à l'aide de la réciprocité quadratique.

Exercice 8

Soit p un nombre premier impair.

1. Montrer que le produit de deux non-carrés modulo p est un carré.
2. Montrer que $x \in \mathbb{Z}$ est un carré modulo p si et seulement si x^5 l'est.

Exercice 9

1. À quelle condition -2 est-il un carré modulo un nombre premier p ? On explicitera le résultat sous forme de congruence modulo 8.
2. Même question en remplaçant -2 par 6 (et en changeant de modulo).

Exercice 10

Calculer les symboles de Jacobi $\left(\frac{7}{15}\right)$, $\left(\frac{7}{45}\right)$, $\left(\frac{11}{45}\right)$, $\left(\frac{30}{77}\right)$, $\left(\frac{55}{273}\right)$.

Exercice 11

1. Calculer $\left(\frac{11}{35}\right)$. 11 est-il un résidu quadratique modulo 35 ?
2. Calculer $\left(\frac{12}{35}\right)$. 12 est-il un résidu quadratique modulo 35 ?
3. Calculer $\left(\frac{18}{35}\right)$. 18 est-il un résidu quadratique modulo 35 ?

Exercice 12

Soit p un nombre premier impair et soit a un nombre entier qui n'est pas multiple de p.

1. Soit ν le nombre d'entiers $i \in \{1, \dots, \frac{1}{2}(p-1)\}$ tels que le reste de la division euclidienne de ai par p soit strictement supérieur à $\frac{1}{2}(p-1)$. Démontrer que $\left(\frac{a}{p}\right) = (-1)^\nu$.
2. Montrer que pour un premier p impair
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{si } p \equiv 1 \text{ ou } -1 \pmod 8 \\ -1 & \text{si } p \equiv 3 \text{ ou } -3 \pmod 8 \end{cases}$$
3. Montrer que pour un premier $p \neq 3$ impair,
$$\left(\frac{3}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{6} \right\rfloor} = \begin{cases} +1 & \text{si } p \equiv 1 \text{ ou } -1 \pmod{12} \\ -1 & \text{si } p \equiv 5 \text{ ou } -5 \pmod{12} \end{cases}$$
4. Montrer que pour un premier $p \neq 5$ impair
$$\left(\frac{5}{p}\right) = (-1)^{\left\lfloor \frac{p+2}{5} \right\rfloor} = \begin{cases} +1 & \text{si } p \equiv 1 \text{ ou } -1 \pmod 5 \\ -1 & \text{si } p \equiv 2 \text{ ou } -2 \pmod 5 \end{cases}$$
5. Montrer que pour un premier $p \neq 7$ impair
$$\left(\frac{7}{p}\right) = \begin{cases} +1 & \text{si } p \equiv 1, 3, 9, 19, 25 \text{ ou } 27 \pmod{28} \\ -1 & \text{si } p \equiv 5, 11, 13, 15, 17 \text{ ou } 23 \pmod{28}. \end{cases}$$

Exercice 13

1. Montrer que si p est un nombre premier congru à 3 modulo 4, et si x est un entier premier à p qui est un carré, alors $x^{\frac{p+1}{4}}$ est une racine carrée de x. Quelle est l'autre ?
2. Trouver, si elles existent, les racines carrées de 3 dans $\mathbb{F}_{113}$.
3. Soit p un nombre premier congru à 1 modulo 4. On écrit $p-1$ sous la forme $2^a m$ où m est un entier impair et a un entier supérieur ou égal à 2. Si z est un non-carré modulo p, alors $z^{\frac{p-1}{2}} = z^{2^{a-1}m} = -1$. En déduire une racine carrée de -1 dans $\mathbb{F}_{113}$.

Exercice 14

Le but de cet exercice est de présenter l'algorithme de Shanks-Tonelli.

Soit p un nombre premier congru à 1 modulo 4. Soit x un entier qui est un carré modulo p. On cherche une racine de x.

1. On écrit $p-1$ sous la forme $2^a m$ où m est un entier impair et a un entier supérieur à 2. On considère $y_1 = x^{\frac{m+1}{2}}$. Alors, $y_1^2 = x^m x = t_1 x$ où on a posé $t_1 = x^m$. Si $t_1 = 1 \pmod p$, y_1 est une racine de x modulo p.
2. Sinon, on considère z un non-carré modulo p. Montrer que z^m est d'ordre 2^a et que $t_1 = x^m$ est aussi d'ordre une puissance 2^{k_1} de 2 mais avec $k_1 < a$.
3. On pose $y_2 = (z^m)^{2^{a-k_1-1}} y_1$. Montrer que $y_2^2 = t_2 x$ où $t_2 = t_1 (z^m)^{2^{a-k_1}}$. Si $t_2 = 1 \pmod p$, y_2 est une racine de x modulo p. Sinon, vérifier que t_2, produit de deux éléments d'ordre 2^{k_1}, est d'ordre une puissance 2^{k_2} de 2 avec $k_2 < k_1$ (combien $\mathbb{F}_p^\times$ a-t-il d'éléments d'ordre 2 ?) En continuant ainsi, on trouvera en moins de a étapes, une racine y_i de x.
4. Trouver, si elles existent, les racines carrées de 2 dans $\mathbb{F}_{113}$.

Exercice 15

Soit p un nombre premier congru à 1 modulo 3.

1. Montrer que le groupe $(\mathbb{F}_p)^\times$ des inversibles du corps $\mathbb{F}_p$ a un élément d'ordre 3.
2. Montrer que le polynôme $X^2 + X + 1$ admet une racine α dans $\mathbb{F}_p$.
3. Vérifier que si d' est un inverse de 2 modulo p, alors $X^2 + X + 1 = (X + d')^2 + 3(d')^2$. En déduire que -3 est un carré dans $\mathbb{F}_p$.
4. Retrouver ce résultat à l'aide de la réciprocité quadratique.

Exercice 16

Soient a, b, c trois entiers n'étant pas des carrés dans $\mathbb{Z}$ tels que abc est un carré dans $\mathbb{Z}$.

Montrer que le polynôme $(X^2-a)(X^2-b)(X^2-c)$ n'a pas de racine dans $\mathbb{Q}$ mais qu'il en a dans $\mathbb{F}_p$, pour tout nombre p premier.

Exercice 17

Soit d un entier relatif sans facteur carré, et soit p un nombre premier de la forme $p = x^2 - dy^2$.

1. Montrer que d est un carré modulo p.
2. On suppose $d = 6$. En déduire que $p = 3$ ou que p vaut $1, -1, 5$ ou -5 modulo 24.

Exercice 18

Soit k un corps fini de cardinal q, et soit un polynôme $P \in k[X]$ de degré $d \geqslant 1$. On suppose que :

(i) P divise $X^{q^d} - X$;

(ii) pour tout diviseur premier p de d, $X^{q^{d/p}} - X$ et P sont premiers entre eux.

Montrer que le polynôme P est irréductible dans $k[X]$.

Exercice 19

Posons $F_n = 2^{2^n} + 1$, pour $n \in \mathbb{N}$.

1. Montrer que $F_n \equiv 2 \pmod 5$ si $n \geqslant 2$.
2. Calculer les symboles de Jacobi $\left(\frac{F_n}{5}\right)$ et $\left(\frac{5}{F_n}\right)$.
3. Montrer que si F_n est premier et $n \neq 1$, alors $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$.
4. On suppose que $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$. Soit p un diviseur premier de F_n, et soit e l'ordre de 5 dans $\mathbb{F}_p^\times$. Montrer que e divise 2^{2^n} mais pas 2^{2^n-1}.
5. Sous les mêmes hypothèses, en déduire que $e = 2^{2^n}$.
6. Sous les mêmes hypothèses, montrer que e divise $p-1$, puis que $p \geqslant F_n$.
7. Montrer que F_n est premier si et seulement si $n = 1$ ou $5^{2^{2^n-1}} \equiv -1 \pmod{F_n}$.