Théorie des nombres
FEUILLE DE TD N○6, CORPS FINIS

1. CALCULS DANS LES CORPS FINIS

Exercice 1

1 Quelle est la caractéristique de $\mathbb{F}_8$, son nombre d'éléments, sa dimension comme espace vectoriel sur un corps premier ?
2 Déterminer un modèle "du" corps fini $\mathbb{F}_8$ sous la forme $(\mathbb{Z}/p\mathbb{Z}[X])/(P)$.
3 Quel est le produit $\Pi_{x\in\mathbb{F}_8}(Y-x)$? Déterminer le $pgcd(Y^8-Y, Y^2+Y+1)$ dans $\mathbb{F}_8[Y]$. Le polynôme Y^2+Y+1 est-il irréductible dans $\mathbb{F}_8[Y]$?
4 Déterminer tous les polynômes $P(Y)$ irréductibles de degré 2 dans $\mathbb{F}_8[Y]$ en cherchant les polynômes de la forme Y^2+aY+b qui n'ont pas de racines dans $\mathbb{F}_8$.

Exercice 2

1 Déterminer tous les polynômes de degré 2 irréductibles dans $\mathbb{F}_2[X]$. Montrer que X^4+X+1 et $X^4+X^3+X^2+X+1$ sont irréductibles dans $\mathbb{F}_2[X]$.
2 Quel est l'ordre de $[X]$ dans $\big(\mathbb{F}_2[X]/X^4+X+1\big)^\times$?
3 Quel est l'ordre de $[x]$ dans $\big(\mathbb{F}_2[x]/x^4+x^3+x^2+x+1\big)^\times$?
4 Déterminer un isomrphisme entre $\mathbb{F}_2[X]/X^4+X+1$ et $\mathbb{F}_2[x]/x^4+x^3+x^2+x+1$.

Exercice 3

1 L'équation $x^2+35y^2=3$ a-t-elle des solutions dans $\mathbb{Z}^2$?
2 L'équation $x^2+3y^2=35$ a-t-elle des solutions dans $\mathbb{Z}^2$?

Exercice 4

1 Résoudre $X^2+X+1=0 \pmod{13}$.
2 Résoudre $X^9=1 \pmod{13}$. On pourra d'abord chercher l'inverse modulo 13 des solutions.

2. NOMBRES PRESQUE PREMIERS

Exercice 5

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 $a^{n-1}=1[n]$.

(1) Trouver tous les entiers b pour lesquels 15 est un nombre pseudopremier.
(2) Pour quelles valeurs de b entre 1 et 91 le nombre 91 est-il pseudopremier ?
(3) Montrer que si p et $2p-1$ sont premiers, alors $n=p(2p-1)$ est pseudopremier pour la moitié des nombres b possibles dans $\{1,\ldots,n\}$, plus précisemment pour ceux qui sont des carrés dans $\mathbf{F}_{2p-1}$.

2 On pose $n=561$. Calculer $\varphi(n)$. Pour quelles valeurs de b entre 1 et 561 le nombre n est-il pseudopremier ?

Exercice 6

1 Montrer que les nombres 1105 $(5\times13\times17)$, 1729 $(7\times13\times19)$ et 2465 $(5\times17\times29)$ 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 7

Soit $b>1$ et p un nombre premier impair ne divisant pas b, $b-1$ ou $b+1$. Soit $n=(b^{2p}-1)/(b^2-1)$.
1 Montrer que $(b^p-1)/(b-1)$ 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 8

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

3. Résidus quadratiques

Exercice 9

1 Montrer que $(2m/n)=(m/n)$ si $n=+/-1$ $[8]$ et $(2m/n)=-(m/n)$ sinon.
2 Vérifier que si m et n sont tous les deux impairs, alors $(m/n)=(n/m)$ sauf si m et n sont tous les deux congrus à 3 $[4]$, auquel cas $(m/n)=-(n/m)$.

Exercice 10

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 $\left(\dfrac{365}{1847}\right)$ à l'aide de la réciprocité quadratique.

Exercice 11

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 12

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 13

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 14

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

4. Calcul de racines carrées

Exercice 15

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 à 2. Si z est un non-carré modulo p, $z^{\frac{p-1}{2}} = y^{2^{a-1}m} = -1$. En déduire une racine de -1 dans $\mathbb{F}_{113}$.

Exercice 16

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 $t_1 = 1[p]$, 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 $t_2 = 1[p]$, 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 $\mathbb{F}_p^\star$ 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 $\mathbb{F}_{113}$.

5. Démonstration de la réciprocité quadratique

Exercice 17

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 $i \in \{1, \ldots, \frac{1}{2}(p-1)\}$ 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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 \text{ si } p \equiv 1 \text{ or } -1 \pmod 8 \\ -1 \text{ si } p \equiv 3 \text{ ou } -3 \pmod 8 \end{cases}$$

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

$$\left(\frac{7}{p}\right) = \begin{cases} +1 \text{ si } p \equiv 1, 3, 9, 19, 25, \text{ ou } 27 \pmod{28} \\ -1 \text{ si } p \equiv 5, 11, 13, 15, 17, \text{ ou } 23 \pmod{28} \end{cases} .$$

6. Application de la réciprocité quadratique

Exercice 18

Soit p un nombre premier congru à 1 modulo 3.

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

Exercice 19

Soient a, b, c trois entiers n'étant pas des carrés dans $\mathbf{Z}$ tels que abc est un carré dans $\mathbf{Z}$. Montrer que le polynôme $(X^2 - a)(X^2 - b)(X^2 - c)$ n'a pas de racine dans $\mathbf{Q}$ mais qu'il en a dans $\mathbf{F}_p$, pour tout nombre p premier.

Exercice 20

On rappelle que $\mathbf{Z}[i\sqrt{2}]$ est factoriel. Le but de l'exercice est de déterminer les nombres premiers p tels que l'équation $x^2 + 2y^2 = p$ ait une solution dans $\mathbf{Z}^2$.

1 Montrer que l'existence d'une solution équivaut au fait que p n'est pas irréductible dans $\mathbf{Z}[i\sqrt{2}]$.
2 Utiliser l'isomorphisme de $\mathbf{Z}[i\sqrt{2}]/(p)$ avec un anneau quotient d'anneau de polynômes, pour montrer que l'existence d'une solution équivaut au fait que -2 est un carré dans $\mathbb{F}_p$ et conclure.

Exercice 21

On rappelle que tout nombre premier congru à 1 modulo 4 est somme de deux carrés. On considère l'équation $x^2 + y^2 = pz^2$ où p est un nombre premier impair.

1 Vérifier qu'elle possède une solution dans $\mathbb{Q}^3$ si et seulement si elle en possède une dans $\mathbb{Z}^3$.
2 Montrer que si elle admet une solution dans $\mathbf{Z}^3 - \{(0,0,0)\}$, -1 est un carré dans $\mathbf{F}_p$ et donc p est congru à 1 modulo 4.
3 La réciproque est-elle vraie ?
4 Lorsqu'elle en possède, décrire toutes les solutions dans $\mathbf{Q}^3$ de l'équation.

Exercice 22

Soit d un entier relatif sans facteur carré. 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 vaut $1, -1, 5,$ ou -5 modulo 24.