*Théorie des nombres*
FEUILLE DE TD N∘4

1. NOMBRES PRESQUE PREMIERS

## Exercice 1

(1) (a) Trouver tous les entiers $b$ pour lesquels 15 est un nombre pseudopremier.
   (b) Pour quelles valeurs de $b$ entre 1 et 91 le nombre 91 est-il pseudopremier ?
   (c) 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) (a) Résoudre $X^9 = 1 \pmod{13}$. On pourra d'abord chercher l'inverse modulo 13 des solutions.
   (b) Pour quelles valeurs de $b$ entre 1 et 91 le nombre 91 est-il fpp ?
   (c) Vérifier que 65 est fpp pour 8 et 18 mais non pour leur produit.
   (d) Soit $n$ un entier divisible par un nombre premier $p$ tel que $p \equiv 3$ [4]. Montrer que si $n$ est fpp pour $a$ et $b$, alors $n$ est fpp pour $ab$.

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

## Exercice 2

**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 3

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 4

**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.

# 2. Utilisation de la réciprocité quadratique

## Exercice 5

**1.**— Calculer les symboles de Legendre suivants :

$$\left(\frac{16}{229}\right), \quad \left(\frac{19}{229}\right), \quad \left(\frac{2}{229}\right), \quad \left(\frac{38}{229}\right).$$

**2.**— Calculer le symbole de Legendre $\left(\frac{365}{1847}\right)$ à l'aide de la réciprocité quadratique.

## Exercice 6

**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).

# 3. Démonstration de la réciprocité quadratique

## Exercice 7

Soit $p$ un nombre premier impair et soit $a$ un nombre entier qui n'est pas multiple de $p$.
**1.**— Soit $\nu$ 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 $(\frac{a}{p}) = (-1)^{\nu}$.
**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

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

## Exercice 8

Soit $p$ un nombre premier congru à 1 modulo 3.
**1.**— Montrer que le groupe $(\mathbf{F}_p)^\times$ des inversibles du corps $\mathbf{F}_p$ admet un élément d'ordre 3.
**2.**— Montrer que le polynôme $X^2 + X + 1$ admet une racine $\alpha$ dans $\mathbf{F}_p$.
**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 $\mathbf{F}_p$.
**4.**— Retrouver ce résultat à l'aide de la réciprocité quadratique.

# 4. Application de la réciprocité quadratique

## Exercice 9

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 10

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 $\mathbf{F}_p$.
**3.**— Conclure.

## Exercice 11

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 $\mathbf{Q}^3$ si et seulement si elle en possède une dans $\mathbf{Z}^3$.
**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 12

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.