CHAPITRE 2

Les carrés et les non-carrés dans $\mathbb{Z}/n\mathbb{Z}$

Exercice 2.1 Soit p un nombre premier impair. Déterminer $\left(\frac{\frac{p+1}{2}}{p}\right)$ et $\left(\frac{\frac{p-1}{2}}{p}\right)$.

Exercice 2.2

1. Déterminer les p premiers pour lesquels l'équation $x^2 \equiv 3 \pmod{p}$ admet au moins une solution ?
2. Pour quels p premiers l'équation $x^2 \equiv 5 \pmod{p}$ a-t-elle des solutions ?

Exercice 2.3 Les nombres 131 et 263 sont premiers. Calculer $O_{263}(131)$ avec un minimum de calculs.

Exercice 2.4 Montrer que les diviseurs premiers de $4n^2+1$ sont de la forme $4k+1$.

Exercice 2.5 Que peut–on dire des diviseurs premiers de $12n^2-1$? Et de $12n^2+1$?

Exercice 2.6

1. $x^2 \equiv 15 \pmod{77}$.
2. Résoudre l'équation $x^2+3\,x+7 \equiv 0 \pmod{115}$

Exercice 2.7 (La méthode de Hensel) Soit p premier impair et a non multiple de p. Démontrer que la congruence $x^2 \equiv a \pmod{p^n}$ admet des solutions si et seulement si $\left(\frac{a}{p}\right) = 1$, et dans ce cas, elle admet exactement 2 solutions modulo p^n.
Application : résoudre $x^2+x+3 \equiv 0 \pmod{125}$.

Exercice 2.8 (Résolution de $x^2 \equiv a \pmod{2^n}$ (a impair))

1. Soit $\alpha \geq 3$, impair. Démontrer que la congruence $x^2 \equiv a \pmod{2^n}$ n'a des solutions que si $a \equiv 1 \pmod 8$.
2. On suppose $a \equiv 1 \pmod 8$. Démontrer que $x^2 \equiv a \pmod 8$ admet exactement 4 solutions modulo 8.
3. On suppose toujours $a \equiv 1 \pmod 8$. Démontrer par récurrence sur n que $x^2 \equiv a \pmod{2^n}$ admet exactement quatre solutions modulo 2^n et expliquer comment les obtenir.

Exercice 2.9 Soit a, b, α entiers avec a *impair* et $\alpha \geq 1$. On s'intéresse à la congruence

$$x^2 + ax + b \equiv 0 \pmod{2^\alpha},$$

1. Démontrer qu'elle n'a pas de solutions si b est impair.
2. Démontrer que si cette congruence admet une solution modulo 2^α alors elle admet exactement deux solutions modulo 2^α.
3. A l'aide de l'exercice précédent prouver que lorsque b est pair elle admet exactement 2 solutions modulo 2^α.

Exercice 2.10 Discuter selon les valeurs de α le nombre de solutions de la congruence

$$x^2 + 4x + 96 \equiv 0 \pmod{2^\alpha}$$

Exercice 2.11

1. Pour quels p premiers l'équation $x^2 + x + 1 = 0 \pmod p$ a-t-elle des solutions ?
2. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ le nombre de solutions de
$$x^2 + x + 1 \equiv 0 \pmod{p^\alpha}$$
3. Quels sont les entiers n pour lesquels $x^2 + x + 1 \equiv 0 \pmod n$ a des solutions ? Discuter le nombre de ces solutions selon la valeur de n

---

Exercice 2.12

1. Pour quels p premiers l'équation $x^2 + 6x + 1 = 0 \pmod p$ a-t-elle des solutions ?
2. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ le nombre de solutions de
$$x^2 + 6x + 1 \equiv 0 \pmod{p^\alpha}$$
3. Quels sont les entiers n pour lesquels $x^2 + 6x + 1 \equiv 0 \pmod n$ a des solutions ? Discuter le nombre de ces solutions selon la valeur de n

---

Exercice 2.13 Montrer que si q et $p = 4q + 1$ sont premiers 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 2.14 Montrer que si p est premier de la forme $4n+1$ alors $n^n \equiv 1 \pmod{p}$.

Exercice 2.15
On appelle $n^{ième}$ nombre de Fermat le nombre $2^{2^n}+1$.

1. Montrer que si un nombre premier est de la forme 2^k+1 alors c'est un nombre de Fermat.
2. Soit $F_n = 2^{2^n}+1$ un nombre de Fermat. Montrer que les diviseurs premiers de F_n sont tous de la forme $k2^{n+1}+1$ (si p est un diviseur premier de F_n, on considèrera l'ordre de 2 modulo p et on montrera qu'il est exactement 2^{n+1}).
3. En considérant le caractère quadratique de 2 modulo p montrer qu'on a un peu mieux : les diviseurs premiers de F_n sont tous de la forme $k2^{n+2}+1$.
4. En marchant sur les traces d'Euler, en déduire que $F_5 = 2^{32}+1 = 4294967297$ n'est pas premier.

Exercice 2.16 Soit $p = F_n = 2^{2^n}+1$, avec $n \geq 1$.

1. On suppose que p est premier.
   (a) Montrer que g est un générateur $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $\left(\frac{g}{p}\right) = -1$.
   (b) Montrer que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Ici on ne suppose pas p premier, mais seulement que
$$3^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$
Montrer que p est premier. Ce test de primalité pour les nombres de Fermat est le test de Pepin.

Exercice 2.17 Soit a un élément *non nul* de $\mathbb{F}_p$. On se propose de démontrer que, pour $x \in \mathbb{F}_p$, les évènements x *est un carré non nul* et $x+a$ *est un carré non nul* sont à peu près indépendants, c'est à dire que le nombre des $x \in \mathbb{F}_p$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$ est environ $\frac{p}{4}$. On note donc A_p le nombre des entiers $x \in \{0, 1, \ldots, p-1\}$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$.

1. Dans le cas où $a = 1$ calculer A_7.
2. On pose $S_p = \sum_{x=0}^{p-1} \left[1 + \left(\frac{x}{p}\right)\right]\left[1 + \left(\frac{x+a}{p}\right)\right]$. Montrer que
$$S_p = 4\,A_p + 2 + \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right).$$
3. On est ainsi ramené au calcul de S_p. Montrer que
$$S_p = p + \sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right).$$

4. Pour $1 \leq x \leq p-1$, soit y l'inverse de x modulo p. Montrer que

$$\left(\frac{x(x+a)}{p}\right) = \left(\frac{1+ay}{p}\right).$$

5. En déduire que $S_p = p-1$, puis la valeur de A_p, et enfin l'encadrement

$$\frac{p-5}{4} \leq A_p \leq \frac{p-1}{4}.$$

Exercice 2.18
(D'après la rubrique de problèmes mathématiques du *Monde*) Soit $(a_1, a_2, \ldots, a_m)$ une suite finie d'entiers. On définit la fonction f qui à tout entier x associe l'entier y défini de la façon suivante : on multiplie a_1 par x et on ajoute a_2. On multiplie le résultat par x et on ajoute a_3, et ainsi de suite, le calcul se terminant après la multiplication par a_{m-1} suivie de l'ajout de a_m.
On suppose que $f(1) = 2$. Le nombre $f(7)$ est-il un carré parfait ?

Exercice 2.19

1. Soit p un nombre premier impair, $k \geq 1$ un nombre entier naturel, $a \in \mathbb{Z}$ non multiple de p et $r \in \mathbb{Z}$ tel que

$$ar \equiv 1 \pmod{p^k}.$$

   On pose $s = r(2-ar)$. Montrer que l'on a

$$as \equiv 1 \pmod{p^{2k}}.$$

   En déduire un algorithme de calcul de l'inverse de a modulo p^n pour $n \in \mathbb{N}^*$.
   Application numérique : calculer l'inverse de 10 modulo $7^3 = 343$.

2. Soit $b \in \mathbb{Z}$ non multiple de p. On rappelle que si le symbole de Legendre $\left(\frac{b}{p}\right)$ est égal à $+1$, la congruence $x^2 \equiv b \pmod{p^n}$ a deux solutions opposées pour tout $n \in \mathbb{N}^*$. Soit $u \in \mathbb{Z}$ et $k \in \mathbb{N}^*$ tels que $u^2 \equiv b \pmod{p^k}$ et soit $v \in \mathbb{Z}$ tel que $uv \equiv 1 \pmod{p^{2k}}$.
   (a) Montrer que p^k divise $u - bv$.
   (b) On pose $w = u + bv$. Montrer que $w^2 \equiv 4b \pmod{p^{2k}}$.
   (c) Déduire de la question précédente un nombre y tel que $y^2 \equiv b \pmod{p^{2k}}$.
3. Donner un algorithme de résolution de la congruence $x^2 \equiv b \pmod{p^n}$ pour $n \in \mathbb{N}^*$.
   Application numérique : Résoudre $x^2 \equiv 2 \pmod{343}$.

Exercice 2.20 (Calcul d'une racine carrée modulo p)
On donne dans cet exercice un algorithme efficace de calcul des racines carrées de a dans $\mathbb{Z}/pZ$ lorsque p est premier impair.

1. Dans la cas ou $p \equiv 3 \pmod 4$ cet algorithme est particulièrement simple. Soit a un carré modulo p. Démontrer que $a^{\frac{p+1}{4}}$ est un racine carrée de a.

2. A partir de maintenant p est un nombre premier impair quelconque. Expliquer comment, en pratique, on peut trouver rapidement un entier b qui ne soit pas un carré modulo p. On choisit un tel entier. On considère alors l'ensemble E des couples (e_1, e_2) satisfaisant
$$a^{e_1} b^{e_2} \equiv 1 \bmod p. \tag{2.1}$$
3. Montrer que $\left(\frac{p-1}{2}, 0\right) \in E$
4. Montrer que si $(e_1, e_2) \in E$ alors e_2 est pair.
5. Montrer que si $(e_1, e_2) \in E$ et si e_1 est impair alors
$$x = a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$
est une racine carrée de a modulo p.
6. Soit $(e_1, e_2) \in E$ avec e_1 pair. Soit $u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}$. Que pouvez vous dire de u^2 ? En déduire un couple $(e'_1, e'_2) \in E$ avec $e'_1 = e_1/2$.
7. En déduire un algorithme de calcul d'une racine carrée de a modulo p. Analyser la complexité de cet algorithme dans le pire des cas, c'est à dire le nombre maximum d'opérations à effectuer pour obtenir ainsi une racine carrée de a. Que se passe-t-il lorsque p est de la forme $p = 4k + 3$?.

Exercice 2.21 (Racines carrées et factorisation)
$N = pq$ est le produit de deux nombres premiers impairs p et q.

1. On suppose connues p et q. Montrer peut on résoudre efficacement l'équation $x^2 \equiv a \pmod N$ à l'aide du théorème des restes chinois et de l'exercice précédent. Ceci prouve que le problème du calcul des racines carrées modulo N n'est pas plus dificile que le problème de la factorisation de N.
2. Dans cette question on montre que le problème du calcul des racines carrées modulo N est aussi difficile que la factorisation de N. Pour cela supposons qu' Alice dispose d'un oracle à qui l'on peut poser autant de fois que l'on veut la question : *a est un carré modulo N. Donnez moi une racine carrée de a modulo N*, et qui répond à chaque fois en renvoyant l'une des racines carrées de a modulo N.

   Expliquez comment, à l'aide cet oracle peut facilement factoriser N.
