# CHAPITRE 6

## Corrigés ou indications : Carrés et non carres

**Exercice 2.8**

1. Pour $p = 2$ on a $x^2 + x + 1 \equiv 1 \pmod 2$ pour tout $x \in \mathbb{F}_2$, et donc $x^2 + x + 1 \equiv 0 \pmod 2$ n'a pas de solution.
   Si $p$ est impair, 4 est premier avec $p$ et la congruence $x^2 + x + 1 \equiv 0 \pmod p$ est équivalente à $4x^2 + 4x + 4 \equiv 0 \pmod p$ soit $(2x+1)^2 \equiv -3 \pmod p$. Elle a des solutions si et seulement si $-3$ est un carré modulo $p$, c'est à dire si et seulement si $p = 3$ ou bien si $\left(\frac{-3}{p}\right) = 1$. Pour $p$ premier impair autre que 3 on a
   $$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{4}} = \left(\frac{p}{3}\right),$$
   et donc $x^2 + x + 1 \equiv 0 \pmod p$ a des solutions si et seulement si $p \equiv 1 \pmod 3$.
2. Pour $p$ premier impair, la congruence
   $$x^2 + x + 1 \equiv 0 \pmod{p^\alpha} \tag{6.1}$$
   s'écrit encore $(2x+1)^2 \equiv -3 \pmod{p^\alpha}$ et ses solutions sont en bijection avec les solutions de
   $$y^2 \equiv -3 \pmod{p^\alpha}.$$
   Lorsque $p = 3$ cette équation admet une unique solution si $\alpha = 1$ qui est $y \equiv 0 \pmod 3$. Si $\alpha \geq 2$ cette congruence implique que $y$ est un multiple de 3, mais alors $-3 \equiv y^2 \pmod{3^\alpha}$ est un multiple de 9 ce qui est absurde. Donc pour $p = 3$ l'unique valeur $\alpha \geq 1$ pour laquelle (6.1) a des solutions est $\alpha = 1$, et dans ce cas l'unique solution est 0 modulo 3.
   Pour $p$ impair avec $p \equiv 1 \pmod 3$, la congruence $x^2 + x + 1 \equiv 0 \pmod p$ a deux solutions, et, par la méthode se Hensel, pour tout $\alpha \geq 1$ la congruence (6.1) a aussi exactement deux solutions.
3. Par le théorème des reste chinois, si $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ est la décomposition en facteurs premiers de $n$, l'ensemble $S$ des solutions de $x^2 + x + 1 \equiv 0 \pmod n$ est en bijection avec le produit $S_1 \times S_2 \times \cdots \times S_k$ ou, pour $j = 1, 2, \ldots, k$, $S_j$ est l'ensemble des solutions de $x^2 + x + 1 \equiv 0 \pmod{q_j^{\alpha_j}}$. Cette équation a donc des solutions si et seulement si $n$ est impair, non divisible par 9, et si les facteurs premiers de $n$ autres que 3 sont tous congrus à 1 modulo 3. De plus si $r$ est le nombre des facteurs premiers impairs de $n$ autre que 3, le nombre des solutions est $2^r$.

**Exercice 2.9**

1. Quel que soit l'entier $n$ la congruence

$$x^2 + 6x + 1 \equiv 0 \pmod{n} \tag{6.2}$$

s'écrit encore

$$(x+3)^2 \equiv 8 \pmod{n}.$$

Si $n = 2$ elle s'écrit $(x+1)^2 \equiv 0 \pmod 2$ et admet l'unique solution $x \equiv 1 \pmod 2$. Si $n = p$, avec $p$ premier impair, elle amet des solutions si et seulement si 8 est un carré modulo $p$, c'est à dire si et seulement si $\left(\frac{8}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)$ est égal à 1 ou encore si $p \equiv \pm 1 \pmod 8$.

2. Pour $p = 2$ la congruence

$$x^2 + 6x + 1 \equiv 0 \pmod{p^\alpha} \tag{6.3}$$

s'écrit encore $(x+3)^2 \equiv 8 \pmod{2^\alpha}$ et ses solutions sont en bijection avec les solutions de

$$y^2 \equiv 8 \pmod{2^\alpha}.$$

   (a) Si $\alpha = 1$ cette équation exactement une solution modulo 2, $y \equiv 0 \pmod 2$.
   (b) Si $\alpha = 2$ cette équation a 2 solutions modulo 4 qui sont les éléments de $\{0, 2\}$.
   (c) Si $\alpha = 3$ cette équation a 2 solutions modulo 8 qui sont les éléments de $\{0, 4\}$.
   (d) Si $\alpha \geq 4$ cette équation n'a pas de solutions, car elle implique $y^2 \equiv 8 \pmod{16}$ et donc $y^2$ multiple de 8 et $y$ multiple de 4 ce qui entraîne $y^2 \equiv 0 \pmod{16}$.

   Pour $p$ impair avec $p \equiv \pm 1 \pmod 8$, la congruence $y^2 \equiv 8 \pmod p$ a deux solutions, et, par la méthode se Hensel, pour tout $\alpha \geq 1$ la congruence (6.3) a aussi exactement deux solutions.

3. Par le théorème des reste chinois, si $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ est la décomposition en facteurs premiers de $n$, l'ensemble $S$ des solutions de $x^2 + 6x + 1 \equiv 0 \pmod n$ est en bijection avec le produit $S_1 \times S_2 \times \cdots \times S_k$ ou, pour $j = 1, 2, \ldots, k$, $S_j$ est l'ensemble des solutions de $x^2 + 6x + 1 \equiv 0 \pmod{q_j^{\alpha_j}}$. L'équation (6.2) a donc des solutions si et seulement si les facteurs premiers impairs de $n$ sont tous congrus à $\pm 1 \pmod 8$, et si $n$ n'est pas divisible par 16.

   Lorsque ces conditions sont satisfaites soit $r$ le nombre des diviseurs premiers impairs de $n$. Le nombre des solutiond de (6.2) est alors $2^r$ si $n$ n'est pas divisible par 4, et $2^{r+1}$ si $n$ est divisible par 4.

**Exercice 2.14**

1. Dans le cas où $a = 1$ calculer $A_7$. Les carrés non nuls modulo 7 sont $\{1, 2, 4\}$. Le seul carré non nul $x$ tel que $x + 1$ soit aussi un carré non nul est $x = 1$, et donc $A_7 = 1$.

2. Si l'un des symboles $\left(\frac{x}{p}\right), \left(\frac{x+a}{p}\right)$ est égal à $-1$ le terme d'indice $x$ dans la somme $S_p$ est nul. Si $x = 0$ le terme d'indice $x$ est égal à $1 + \left(\frac{a}{p}\right)$. Si $x = -a$ le terme d'indice $x$ est égal à $1 + \left(\frac{-a}{p}\right)$. Les termes restants sont ceux pour lesquels $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$. Ils sont au nombre de $A_p$, et chacun prend la valeur $2 \times 2 = 4$. D'où $S_p = 4\,A_p + 2 + \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right)$.
3. En développant le terme d'indice $x$ dans la somme $S_p$ on obtient
$$S_p = \sum_{x=0}^{p-1} 1 + \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) + \sum_{x=0}^{p-1} \left(\frac{a+x}{p}\right) + \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{a+x}{p}\right)$$
La première somme vaut $p$, la deuxième et la troisième sont nulles, et la dernière, en utilisant la multiplicativité du symbole de Legendre, s'écrit encore
$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{a+x}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x(x+a)}{p}\right),$$
d'où $S_p = p + \sum_{x=0}^{p-1} \left(\frac{x(x+a)}{p}\right) = p + \sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right)$.
4. Pour $1 \leq x \leq p-1$, soit $y$ l'inverse de $x$ modulo $p$. Alors
$$\begin{aligned}\left(\frac{x(x+a)}{p}\right) &= \left(\frac{xxy(x+a)}{p}\right) = \left(\frac{x^2}{p}\right)\left(\frac{y(x+a)}{p}\right) \\ &= \left(\frac{yx+ay}{p}\right) = \left(\frac{1+ay}{p}\right)\end{aligned}$$
5. Quand $x$ décrit l'ensemble $\mathbb{F}_p^*$, il en est de même de son inverse $y$, et, par la question précédente on a
$$\sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{1+ay}{p}\right).$$
Comme $a$ est inversible modulo $p$, l'application $y \to 1+ay$ est une bijection de $\mathbb{F}_p$ sur $\mathbb{F}_p$. L'image de 0 par cette bijection est 1. Il en résulte que, lorsque $y$ prend les valeurs $1, 2, \ldots, p-1$, $1+ay$ prend toutes les valeurs de $\mathbb{F}_p$, sauf la valeur 1, et on a
$$\sum_{y=1}^{p-1} \left(\frac{1+ay}{p}\right) = \sum_{u=0}^{p} \left(\frac{u}{p}\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1.$$
La question (3) donne alors $S_p = p-1$, et enfin, par la question (2)
$$A_p = \frac{1}{4}\left[p - 3 - \left(\frac{a}{p}\right) - \left(\frac{-a}{p}\right)\right].$$
Comme la somme $\left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right)$ est comprise entre $-2$ et 2, on en déduit
$$\frac{p-5}{4} \leq A_p \leq \frac{p-1}{4}.$$
Remarquons que, lorsque $p$ est de la forme $p = 4k+3$, la seule valeur entière de l'intervalle ci dessus est $\frac{p-3}{4}$, et donc $A_p = \frac{p-3}{4}$.