UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen — Seconde session — corrigé

Exercice 1

Le but de cet exercice est de montrer que si $n > 2$ est un entier impair et $a \in \mathbb{Z}$, alors on ne peut pas avoir $a^{n-1} \equiv -1 \pmod{n}$.

On note ici v_2 la valuation 2-adique : si $x \in \mathbb{Z} \setminus \{0\}$, alors $v_2(x)$ est le plus grand entier $v \geqslant 0$ tel que $2^v \mid x$.

Dans toute la suite de l'exercice, n désigne un entier impair > 2 et a un entier.

Question 1

Soit p un nombre premier impair. On suppose qu'il existe un entier $k \geqslant 0$ tel que $a^k \equiv -1 \pmod{p}$. On note e l'ordre de a dans $\mathbb{F}_p^\times$. Montrer que $e \mid (2k)$ et $e \nmid k$.

Notons que la relation $a^k \equiv -1 \pmod{p}$ implique que $a \not\equiv 0 \pmod{p}$, donc a donne bien un élément de $\mathbb{F}_p^\times$ par réduction modulo p.

Comme e est l'ordre de a dans $\mathbb{F}_p^\times$, on a $a^t \equiv 1 \pmod{p}$ si et seulement si $e \mid t$.

Ici, on a $a^k \equiv -1 \not\equiv 1 \pmod{p}$ (car $p \neq 2$), donc $e \nmid k$, et $a^{2k} \equiv (-1)^2 \equiv 1 \pmod{p}$ donc $e \mid (2k)$.

Question 2

En déduire que $v_2(e) = 1 + v_2(k)$.

Considérons la décomposition de k et de e en produit de facteurs premiers :

$$k = \prod_{\pi \text{ premier}} \pi^{v_\pi(k)} \qquad \text{et} \qquad e = \prod_{\pi \text{ premier}} \pi^{v_\pi(e)}.$$

Comme $e \mid (2k)$, on a $v_2(e) \leqslant v_2(2k) = 1 + v_2(k)$, et $v_\pi(e) \leqslant v_\pi(2k) = v_\pi(k)$ pour tout π premier impair. Si l'on avait $v_2(e) < 1 + v_2(k)$, alors on aurait $v_2(e) \leqslant v_2(k)$, donc $e \mid k$, ce qui est faux. Donc $v_2(e) = 1 + v_2(k)$.

Question 3

En déduire que $p \equiv 1 \pmod{2^{1+v_2(k)}}$.

D'après la question précédente, on a $2^{1+v_2(k)} \mid e$. Or e est l'ordre de a dans le groupe $\mathbb{F}_p^\times$, qui a $p-1$ éléments, donc $e \mid (p-1)$, donc $2^{1+v_2(k)} \mid (p-1)$, i.e. $p \equiv 1 \pmod{2^{1+v_2(k)}}$.

Question 4

On suppose maintenant qu'il existe un entier $k' \geqslant 0$ tel que $a^{k'} \equiv -1 \pmod{n}$. Montrer que $n \equiv 1 \pmod{2^{1+v_2(k')}}$.

Soit $n = \prod_{i \in I} p_i$ la décomposition de n en produit de facteurs premiers (avec p_i premiers pas forcément distincts). Pour tout $i \in I$, on a $a^{k'} \equiv -1 \pmod{p_i}$ (car $p_i \mid n$), et p_i est un nombre premier impair (car n est impair. La question précédente donne alors $p_i \equiv 1 \pmod{2^{1+v_2(k')}}$.

Ceci étant vrai pour tous les i, on trouve $n \equiv \prod_{i \in I} 1 \equiv 1 \pmod{2^{1+v_2(k')}}$.

Question 5

En déduire qu'on ne peut pas avoir $a^{n-1} \equiv -1 \pmod{n}$.

Si l'on avait $a^{n-1} \equiv -1 \pmod{n}$, alors la question précédente (avec $k' = n-1$) donnerait $n \equiv 1 \pmod{2^{1+v_2(n-1)}}$, c'est-à-dire $v_2(n-1) \geqslant 1 + v_2(n-1)$, ce qui est impossible.

On ne peut donc pas avoir $a^{n-1} \equiv -1 \pmod{n}$.

Exercice 2

Question 1

Montrer qu'il n'y a qu'une seule forme quadratique en deux variables à cœfficients entiers, $aX^2 + bXY + cY^2$, positive et de discriminant -3, qui soit réduite.

Rappelons que l'on dit qu'une forme quadratique $aX^2 + bXY + cY^2$, de discriminant $\Delta = b^2 - 4ac < 0$, est réduite si :

(i) $|b| \leqslant a \leqslant c$

(ii) de plus, si ($|b| = a$ ou $a = c$ alors $b \geqslant 0$.

On a alors $0 \leqslant a \leqslant c$ donc $a^2 \leqslant ac$, et $b^2 \leqslant a^2$, donc $b^2 - 4ac \leqslant -3a^2$, donc $0 \leqslant a \leqslant \sqrt{\frac{-\Delta}{3}}$.

Les formes (positives) réduites de discriminant $\Delta = -3$ vérifient donc $0 \leqslant a \leqslant 1$. Avec $a = 0$, on aurait $b^2 = \Delta = -3$, ce qui est impossible. Donc $a = 1$. Comme $|b| \leqslant a = 1$, on a $b = 0$ ou $b = \pm 1$. Si $b = 0$, on aurait $-4c = \Delta = -3$, ce qui est impossible. Donc $b = \pm 1$,

donc on est dans le cas $|b| = a$, donc $b \geqslant 0$, donc $b = 1$. On a donc $-3 = \Delta = 1 - 4c$, donc $c = 1$.

Il y a donc une unique forme quadratique positive réduite de discriminant -3, et cette forme est $X^2 + XY + Y^2$.

Question 2

En déduire que la forme $X^2 + XY + Y^2$ représente proprement un entier $N > 0$ si et seulement si -3 est un carré modulo $4N$. (Indication : on pourra considérer une forme qui représente N au point $(X, Y) = (1, 0)$).

La forme (primitive) $X^2 + XY + Y^2$ représente proprement l'entier N si et seulement si elle est équivalente à une forme primitive $NX^2 + \beta XY + \gamma Y^2$. Comme il n'y a qu'une seule forme positive réduite (d'après la question précédente) et donc une seule classe d'équivalence de formes quadratiques positives de discriminant -3, cela équivaut à l'existence d'une forme quadratique $NX^2+\beta XY+\gamma Y^2$ de discriminant -3, i.e. à l'existence d'entiers β et γ tels que $\beta^2 - 4N\gamma = -3$, i.e. à ce que -3 soit un carré modulo $4N$.

Question 3

Soit p un nombre premier impair. Déduire de la question précédente qu'il existe $x, y \in \mathbb{Z}$ tels que $x^2 + xy + y^2 = p$ si et seulement si $p = 3$ ou $p \equiv 1 \pmod 3$.

Comme p est premier, il ne peut être représenté que proprement. D'après la question précédente, on obtient donc qu'il existe $x, y \in \mathbb{Z}$ tels que $x^2 + xy + y^2 = p$ si et seulement si -3 est un carré modulo $4p$.

Par le théorème chinois, cette condition équivaut à ce que -3 soit un carré modulo 4 et modulo p. Comme -3 est un carré modulo 4 (c'est 1^2), cela équivaut à $\left(\frac{-3}{p}\right) = 0$ ou 1.

Finalement, on a :

$$\begin{aligned}\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{(3-1)(p-1)}{4}}\left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \\ &= \begin{cases} 0 & \text{si } p = 3 \\ 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv -1 \pmod 3. \end{cases}\end{aligned}$$

On trouve donc bien qu'il existe $x, y \in \mathbb{Z}$ tels que $x^2 + xy + y^2 = p$ si et seulement si $p = 3$ ou $p \equiv 1 \pmod 3$.

Exercice 3

Le but de cet exercice est de résoudre l'équation diophantienne $x^2 + 2 = 3^n$ (avec $x \geqslant 0$ et $n \geqslant 0$ entiers).
On note $K = \mathbb{Q}(\sqrt{-2})$. Rappelons que l'anneau des entiers de K est $\mathscr{O}_K = \mathbb{Z}[\sqrt{-2}]$, et que c'est un anneau euclidien.

Question 1

On considère x et n vérifiant l'équation. Montrer que x et n sont impairs. (Indication : on pourra réduire modulo 4).

En réduisant modulo 4 l'équation $x^2 + 2 = 3^n$, on trouve $x^2 + 2 \equiv (-1)^n \pmod 4$. Comme x^2 est congru à 0 ou 1 modulo 4, et $(-1)^n$ vaut -1 ou 1, la congruence n'est possible que si $x \equiv 1 \pmod 4$ et $(-1)^n = -1$, c'est-à-dire si x et n sont impairs.

Question 2

Décomposer 3^n en produit d'irréductibles de l'anneau $\mathscr{O}_K$.

Notons que l'anneau $\mathscr{O}_K$ est factoriel (puisqu'il est euclidien), donc cette décomposition en produit d'irréductibles existe et (surtout) est unique à permutation près et multiplications par des unités près.
On a $3 = (1 - \sqrt{-2})(1 + \sqrt{-2})$ dans $\mathscr{O}_K$. Montrons que c'est la décomposition de 3 en produit d'irréductibles.
Comme $N_{K/\mathbb{Q}}(1 - \sqrt{-2}) = N_{K/\mathbb{Q}}(1 - \sqrt{-2}) = 3$ est premier, $1 - \sqrt{-2}$ et $1 + \sqrt{-2}$ sont irréductibles dans $\mathscr{O}_K$.
Les inversibles de $\mathscr{O}_K$ sont les éléments de norme ± 1, donc de norme 1 (puisqu'ici le norme est positive), c'est-à-dire 1 et -1, donc $1 - \sqrt{-2}$ et $1 + \sqrt{-2}$ ne sont pas associés.
Par élévation à la puissance n, on en déduit que la décomposition de 3^n en produit d'irréductibles est (à permutation près et à multiplications par ± 1 près) :

$$3^n = \left(1 - \sqrt{-2}\right)^n \left(1 + \sqrt{-2}\right)^n.$$

Question 3

Montrer que $x + \sqrt{-2}$ et $x - \sqrt{-2}$ sont premiers entre eux dans l'anneau $\mathscr{O}_K$.

On considère un diviseur commun $d \in \mathscr{O}_K$ de ces deux éléments. Comme il divise leur différence, on a $d \mid 2\sqrt{-2}$ donc $N_{K/\mathbb{Q}}(d) \mid 8$. D'autre part, comme $d \mid (x + \sqrt{-2})$ et $N_{K/\mathbb{Q}}(x + \sqrt{-2}) = x^2 + 2 = 3^n$, on a $N_{K/\mathbb{Q}}(d) \mid 3^n$. Comme $8 = 2^3$ et 3^n sont premiers entre

eux (dans $\mathbb{Z}$), on a $N_{K/\mathbb{Q}}(d) = 1$, i.e. d est inversible. Donc $x + \sqrt{-2}$ et $x - \sqrt{-2}$ sont premiers entre eux.

Question 4

En déduire qu'il existe $\varepsilon_0, \varepsilon_1 \in \{\pm 1\}$ tels que $x - \sqrt{-2} = \varepsilon_0(1 - \varepsilon_1\sqrt{-2})^n$. (Les propriétés de l'anneau $\mathscr{O}_K$ employées devront être mentionnées explicitement).

Rappelons que les unité de $\mathscr{O}_K$ sont ± 1 (cf. réponse à la question 2).
D'après la question 2, on a

$$(x - \sqrt{2})(x + \sqrt{2}) = 3^n = (1 - \sqrt{-2})^n(1 + \sqrt{-2})^n,$$

le produit de droite étant formé de facteurs irréductibles.
Comme l'anneau $\mathscr{O}_K$ est factoriel, par unicité de la factorisation, on trouve

$$\begin{aligned} x - \sqrt{-2} &= \varepsilon_0(1 - \sqrt{-2})^e(1 + \sqrt{-2})^f \\ x + \sqrt{-2} &= \varepsilon_0^{-1}(1 - \sqrt{-2})^{f'}(1 + \sqrt{-2})^{e'}, \end{aligned}$$

avec $e, f, e', f' \geqslant 0$ des entiers tels que $e + f' = n$ et $f + e' = n$ et $\varepsilon_0 \in \{\pm 1\}$ une unité.
Par conjugaison de la première égalité et unicité de la factorisation, on a $e = e'$ et $f = f'$.
D'autre part, comme $x - \sqrt{-2}$ et $x + \sqrt{-2}$ sont premiers entre eux (d'après la question précédente), on a $\min(e, f) = 0$. On a donc deux possibilité : $e = n$ et $f = 0$, ou $e = 0$ et $f = n$, c'est-à-dire $x - \sqrt{-2} = \varepsilon_0(1 - \varepsilon_1\sqrt{-2})$, avec $\varepsilon = 1$ dans le premier cas et $\varepsilon_1 = -1$ dans le second.

Question 5

On pose $a = 1 + \sqrt{-2}$ et $b = 1 - \sqrt{-2}$. Montrer que $a = 2 - b$, $\sqrt{-2} = 1 - b$, $2x = \varepsilon_0(a^n + b^n)$ et $-2\sqrt{-2} = \varepsilon_0\varepsilon_1(a^n - b^n)$.

On a :

$$\begin{aligned} 2 - b &= 2 - (1 - \sqrt{-2}) \\ &= 1 + \sqrt{-2} \\ &= a \\ 1 - b &= 1 - (1 - \sqrt{-2}) \\ &= \sqrt{-2} \\ 2x &= (x - \sqrt{-2}) + (x + \sqrt{-2}) \\ &= \varepsilon_0 \begin{cases} a^n + b^n & \text{si } \varepsilon_1 = 1 \\ b^n + a^n & \text{si } \varepsilon_1 = -1 \end{cases} \\ &= \varepsilon_0(a^n + b^n) \end{aligned}$$

$$\begin{aligned} -2\sqrt{-2} &= (x-\sqrt{-2})-(x+\sqrt{-2}) \\ &= \varepsilon_0 \begin{cases} a^n - b^n & \text{si } \varepsilon_1 = 1 \\ b^n - a^n & \text{si } \varepsilon_1 = -1 \end{cases} \\ &= \varepsilon_0\varepsilon_1(a^n+b^n) \end{aligned}$$

Question 6

Montrer que l'anneau $\mathscr{O}_K/b\mathscr{O}_K$ est isomorphe à $\mathbb{F}_3$.

Dans $\mathbb{Z}[X]$, on a $X^2+2=(1-X)(-1-X)+3$, donc $\{X^2+2, 1-X\}$ et $\{1-X, 3\}$ engendrent le même idéal, d'où les isomophismes

$$\begin{array}{ccccccc} \mathscr{O}_K/b\mathscr{O}_K & \xleftarrow{\sim} & \mathbb{Z}[X]/(X^2+2, 1-X) = \mathbb{Z}[X]/(1-X, 3) & \xrightarrow{\sim} & \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3 \\ \sqrt{-2} & \longmapsto & X & \longmapsto & 1. \end{array}$$

On peut aussi remarquer que $\mathscr{O}_K/b\mathscr{O}_K$ est un anneau à $N_{K/\mathbb{Q}}(b)=3$ éléments, et que le seul anneau commutatif unitaire à 3 éléments est $\mathbb{F}_3$.

Question 7

Montrer que $\varepsilon_0\varepsilon_1 = 1$. (Indication : utiliser les résultats des deux questions précédentes). En déduire que $-2\sqrt{-2} = a^n - b^n$.

En appliquant l'isomorphisme de la question précédente à l'égalité $-2\sqrt{-2} = \varepsilon_0\varepsilon_1(a^n-b^n)$, on trouve $-2 = \varepsilon_0\varepsilon_1(2^n-0)$ dans $\mathbb{F}_3$, c'est-à-dire, comme n est impair, $1 \equiv \varepsilon_0\varepsilon_1 \pmod 3$. Comme $\varepsilon_0, \varepsilon_1 \in \{\pm 1\}$, on en déduit $\varepsilon_0\varepsilon_1 = 1$.
Finalement, comme $-2\sqrt{-2} = \varepsilon_0\varepsilon_1(a^n-b^n)$, on trouve bien $-2\sqrt{-2} = a^n - b^n$.

Question 8

Montrer que $a^{2^v} \equiv 1-2^v(\sqrt{-2}+2) \pmod{2^{v+2}}$ dans $\mathscr{O}_K$, pour tout entier $v \geqslant 2$. (Indication : procéder par récurrence sur v, à l'aide de la formule de binôme).

Pour $v=2$, on a :

$$a^{2^v} = (1+\sqrt{-2})^4 = (-1+2\sqrt{-2})^2 = -7-4\sqrt{-2} = 1-2^v(\sqrt{-2}+2),$$

donc la congruence est vraie.
Supposons maintenant que $a^{2^v} \equiv 1-2^v(\sqrt{-2}+2) \pmod{2^{v+2}}$ pour un entier $v \geqslant 2$ donné. Il existe alors un $r \in \mathbb{Z}$ tel que

$$a^{2^v} = 1-2^v(\sqrt{-2}+2+4r),$$

d'où :

$$\begin{aligned} a^{2^{v+1}} &= 1 - 2^{v+1}(\sqrt{-2} + 2 + 4r) + 2^{2v}(\sqrt{-2} + 2 + 4r)^2 \\ &= 1 - 2^{v+1}(\sqrt{-2} + 2 + 4r) - 2^{2v+1}(1 - \sqrt{-2} - 2r\sqrt{-2})^2 \\ &\equiv 1 - 2^{v+1}(\sqrt{-2} + 2) \pmod{2^{v+3}} \quad \text{puisque } v \geqslant 2, \end{aligned}$$

d'où la récurrence.

Question 9

On considère maintenant deux solutions x_0, n_0 et x_1, n_1 de l'équation diophantienne, avec $n_1 > n_0$. On note v le plus grand entier tel que $2^v \mid (n_1 - n_0)$, et on suppose $v \geqslant 2$. Montrer que $a^{n_1 - n_0} \equiv 1 + (n_1 - n_0)(\sqrt{-2} + 2) \pmod{2^{v+2}}$.

Posons $k = 2^{-v}(n_1 - n_0)$. On a :

$$\begin{aligned} a^{n_1 - n_0} &= a^{2^v k} \\ &\equiv \left(1 - 2^v(\sqrt{-2} + 2)\right)^k \pmod{2^{v+2}} \\ &\equiv 1 - 2^v k(\sqrt{-2} + 2) + \sum_{i=2}^{k} (-1)^i \binom{k}{i} 2^{vi}(\sqrt{-2} + 2)^i \pmod{2^{v+2}} \\ &\equiv 1 - 2^v k(\sqrt{-2} + 2) \pmod{2^{v+2}} \quad \text{car } v \geqslant 2, \end{aligned}$$

d'où le résultat annoncé.

Question 10

En déduire que $a^{n_1} \equiv a^{n_0} + (n_1 - n_0)(\sqrt{-2} + 2)a^{n_0} \pmod{2^{v+2}}$, puis, en calculant $a^{n_1} - b^{n_1}$, que $0 \equiv 2(n_1 - n_0)(\varepsilon_0 x_0 - 2)\sqrt{-2} \pmod{2^{v+2}}$.

D'après la question précédente, on a $a^{n_1 - n_0} \equiv 1 + (n_1 - n_0)(\sqrt{-2} + 2) \pmod{2^{v+2}}$, donc, en multipliant par a^{n_0} :

$$a^{n_1} \equiv a^{n_0} + (n_1 - n_0)(\sqrt{-2} + 2)a^{n_0} \pmod{2^{v+2}}.$$

Par conjugaison, on en déduit :

$$b^{n_1} \equiv b^{n_0} + (n_1 - n_0)(-\sqrt{-2} + 2)b^{n_0} \pmod{2^{v+2}},$$

donc

$$a^{n_1} - b^{n_1} \equiv a^{n_0} - b^{n_0} + (n_1 - n_0)\left((a^{n_0} + b^{n_0})\sqrt{-2} + 2(a^{n_0} - b^{n_0})\right) \pmod{2^{v+2}}.$$

Comme $-2\sqrt{-2} = a^{n_0} - b^{n_0} = a^{n_1} - b^{n_1}$ (cf. question 7) et $2\varepsilon_0 x_0 = a^{n_0} + b^{n_0}$ (cf. question 5, en se rappelant que $\varepsilon_0 = \pm 1$), on trouve

$$\begin{aligned} 0 &\equiv (n_1 - n_0)\left(2\varepsilon_0 x_0\sqrt{-2} - 4\sqrt{-2}\right) \pmod{2^{v+2}} \\ &\equiv 2(n_1 - n_0)(\varepsilon_0 x_0 - 2)\sqrt{-2} \pmod{2^{v+2}}. \end{aligned}$$

Question 11

En déduire que $2^{v+1} \mid (n_1 - n_0)$, que qui contredit la définition de v. Montrer que chaque classe de congruence modulo 4 contient au plus un entier $n \geqslant 0$ tel que $3^n - 2$ soit un carré.

D'après la question précédente, on a $2^{v+1} \mid (n_1 - n_0)(\varepsilon_0 x_0 - 2)\sqrt{-2}$ dans $\mathscr{O}_K$, donc $2^{v+1} \mid (n_1 - n_0)(\varepsilon_0 x_0 - 2)$ dans $\mathbb{Z}$. Or x_0 est impair (question 1), donc $\varepsilon_0 x_0 - 2$ aussi, donc $2^{v+1} \mid (n_1 - n_0)$. Comme 2^v est la puissance de 2 de plus grand exposant qui divise $n_1 - n_0$, on a une contradiction.

On ne peut donc pas avoir deux solutions x_0, n_0 et x_1, n_1 telles que $4 \mid (n_1 - n_0)$, c'est-à-dire deux entiers n_0 et n_1 dans la même classe de congruence modulo 4 tels que $3^{n_0} - 2$ et $3^{n_1} - 2$ soient des carrés. Il y a donc au plus un tel entier dans chaque classe de congruence.

Question 12

Quelles sont les solutions de l'équation $x^2 + 2 = 3^n$, avec x et n des entiers positifs ? (La réponse doit bien sûr être démontrée).

D'après la question 1, si x, n est solution, on a $x \equiv 1 \pmod 4$ ou $x \equiv 3 \pmod 4$. Or, chacune de ces deux classes de congruence contient une solution : $1^2 + 2 = 3^1$ ($n = 1$) et $5^2 + 2 = 3^3$ ($n = 3$). D'après la question précédente et la relation $x = \sqrt{3^n - 2}$, ce sont les seules solutions de l'équation.

Les solutions de $x^2 + 2 = 3^n$, avec $x, n \geqslant 0$ entiers, sont $x = 1, n = 1$ et $x = 5, n = 3$.