

**Devoir surveillé n°4**  
**CORRECTION**

---

**Exercice : Suite**      **/14**

On note  $I = [-\frac{4}{3}, +\infty[$  et  $f : x \mapsto \sqrt{3x+4}$ .

1.  $f$  est définie sur  $\{x \in \mathbb{R} \mid 3x+4 \geq 0\} = I$

Puis, comme  $t \mapsto 3t+4$  et  $\sqrt{\phantom{x}}$  sont croissantes, par composition

/1

$f$  est croissante sur  $I$  et  $f(I) = \mathbb{R}_+ \subset I$ .

On considère la suite  $(u_n)$  définie par récurrence par  $u_0 \in I$  et pour tout  $n \in \mathbb{N}$ ,  $u_{n+1} = f(u_n)$ .

2. Si  $(u_n)$  converge vers  $\ell$ , alors  $\ell$  vérifie  $f(\ell) = \ell$  et donc  $3\ell+4 = \ell^2$ .

Or le polynôme se factorise :  $\ell^2 - 3\ell - 4 = (\ell-4)(\ell+1)$ .

/1

Si  $(u_n)$  converge vers  $\ell$ , alors  $\ell \in \{-1, 4\}$ .

3. Puisque  $f$  est croissante sur  $I$ , la suite  $(u_n)$  est monotone.

Son sens de variation dépend des premières valeurs.

Pour tout  $x \in I$ , on a les équivalences suivantes.

$$f(x) - x \geq 0 \iff f(x) \geq x \iff \sqrt{3x+4} \geq x$$

- Si  $x < 0$ , ce résultat est toujours vrai, car  $\sqrt{3x+4} \geq 0 \geq x$ .
- Si  $x \geq 0$ , on a encore les équivalences :

$$f(x) - x \geq 0 \iff 3x+4 \geq x^2 \iff (x-4)(x+1) \leq 0 \iff x \leq 4$$

Donc si  $u_0 \geq 4$ , alors  $f(u_0) - u_0 \leq 0$ , donc  $u_1 \leq u_0$ .

puis par monotonie de  $(u_n)$ ,  $(u_n)$  est décroissante.

Donc si  $u_0 \leq 4$ , alors  $f(u_0) - u_0 \geq 0$ , donc  $u_1 \geq u_0$ .

puis par monotonie de  $(u_n)$ ,  $(u_n)$  est croissante.

/2

Si  $u_0 \leq 4$ ,  $(u_n)$  est croissante et si  $u_0 \geq 4$ ,  $(u_n)$  est décroissante.

4. Pour le second cas,  $(u_n)$  est également minorée par 0, donc elle converge et sa limite est positive.

Il ne peut s'agir que de 4.

Pour le premier cas, comme  $f$  est croissante sur  $[-\frac{4}{3}, 4]$ ,  $f([-\frac{4}{3}, 4]) = [f(-\frac{4}{3}), f(4)] = [0, 4]$ ,

$[-\frac{4}{3}, 4]$  est stable par  $f$ , donc pour tout  $n \in \mathbb{N}$ ,  $u_n \leq 4$ .

Donc  $(u_n)$  est croissante majorée donc convergente.  $u_1 \geq 0$ , donc  $\lim(u_n) \geq 0$ ,  $\lim(u_n) \neq -1$ .

Dans ce cas,  $(u_n)$  converge également vers 4.

/2

Dans tous les cas (quelle que soit la valeur de  $u_0$ ),  $(u_n)$  converge vers 4.

**Problème. Réciprocité quadratique**

**Préliminaires**

Soit  $p \in \mathbb{N}$ , un nombre premier.

1. Soit  $t_n : x \mapsto \sum_{k=0}^n a_k x^k$ , polynomiale à coefficients entiers de degré  $n$ .

On suppose qu'il existe  $a \in \mathbb{Z}$  tel que  $t_n(a) \equiv 0[p]$ .

Pour tout  $x \in \mathbb{Z}$  :

$$t_n(x) - t_n(a) = \sum_{k=1}^n a_k (x^k - a^k) + a_0 - a_0 = \sum_{k=1}^n \left( (x-a) a_k \sum_{h=0}^{k-1} x^{k-1-h} a^h \right) = (x-a) \underbrace{\sum_{k=1}^n a_k \sum_{h=0}^{k-1} x^{k-1-h} a^h}_{p_{n-1}(x)}$$

Soit  $k \in \llbracket 1, n-1 \rrbracket$

Comme pour tout  $h \in \llbracket 0, k-1 \rrbracket$ ,  $k-1-h \leq k-1$ , alors  $\deg \left( \sum_{h=0}^{k-1} x^{k-1-h} a^h \right) \leq k-1$ .

Donc  $\deg t_{n-1} \leq \max\{k-1, k \in \llbracket 1, n \rrbracket\} \leq n-1$ .

Enfin, comme  $t_n(a) \equiv 0[p]$ , on plonge la relation modulo  $p$  :

/3

il existe  $t_{n-1}$ , polynomiale à coefficients entiers et de degré au plus  $n-1$  telle que  
 $\forall x \in \mathbb{Z}, t_n(x) \equiv (x-a)t_{n-1}(x)[p]$ .

2. Soit  $t_n : x \mapsto \sum_{k=0}^n a_k x^k$ , polynomiale à coefficients entiers de degré  $n$ .

On démontre par récurrence pour  $k \leq n$  :

$\mathcal{P}_k$  :  $\ll$  Si il existe  $a_1, a_2, \dots, a_k$  distincts de  $\llbracket 0, p-1 \rrbracket$ , tels que  $t_n(a_k) \equiv 0[p]$   
 alors, il existe  $t_{n-k}$  polynomiale de degré au plus  $n-k$  telle que

$$\forall x \in \mathbb{Z}, t_n(x) \equiv \prod_{i=1}^k (x-a_i) \times t_{n-k}(x)[p] \gg$$

—  $\mathcal{P}_0$  est vraie. avec  $t_{n-0} = p_n$ .

—  $\mathcal{P}_1$  est vraie d'après la question précédente (mais cela ne joue aucun rôle dans la démonstration de la récurrence).

— Soit  $k < n$ . Supposons que  $\mathcal{P}_k$  est vraie.

Supposons, qu'il existe  $k+1$  nombres (distincts)  $a_1, \dots, a_k, a_{k+1}$  de  $\llbracket 0, p-1 \rrbracket$  tels que :  
 $t_n(a_k) \equiv 0[p]$ .

On peut alors appliquer  $\mathcal{P}_k$  pour les nombres  $a_1, \dots, a_k$ .

Donc il existe  $t_{n-k}$ , polynomiale de degré au plus  $n-k$ , tel que

$$\forall x \in \mathbb{Z}, t_n(x) \equiv \prod_{i=1}^k (x-a_i) \times t_{n-k}(x)[p].$$

Puis  $t_n(a_{k+1}) \equiv 0[p]$ , donc  $\prod_{i=1}^k (a_{k+1} - a_i) \times t_{n-k}(a_{k+1}) \equiv 0[p]$

Or  $p$  est premier donc divise l'un des termes.

Mais pour tout  $i \in \mathbb{N}_k$ ,  $a_{k+1} - a_i \in \llbracket -p+1, p-1 \rrbracket \setminus \{0\}$  car  $a_{k+1} \neq a_i$ .

Donc  $t_{n-k}(a_{k+1}) \equiv 0[p]$ .

Ainsi, d'après q.1 (en adaptant  $n$ ), il existe  $t_{n-k-1}$  de degré inférieur à  $\deg(t_{n-k} - 1)$  tq  
 pour tout  $x \in \mathbb{Z}, t_{n-k}(x) \equiv (x-a_{k-1})t_{n-k-1}(x)[p]$

On ré-injecte dans la formule précédente, et on trouve que  $\mathcal{P}_{k+1}$  est vraie.

Supposons maintenant que  $t_n$  admette  $n$  racines distincts :  $a_1, \dots, a_n$  de  $\llbracket 0, p-1 \rrbracket$

alors il existe un polynôme  $t_0$  de degré au plus 0 tel que

$$\forall x \in \mathbb{Z}, t_n(x) \equiv t_0(x) \prod_{i=1}^n (x-a_i)[p].$$

Comme  $t_0$  est une constante, on a  $t_n(x) \equiv 0[p]$  si et seulement si  $\exists i \in \mathbb{N}_n$  tel que  $p|x-a_i$ .

Donc, si par ailleurs  $x \in \llbracket 0, p-1 \rrbracket$ ,  $x \in \{a_1, \dots, a_n\}$ .

/3

$t_n$  ne peut admettre plus de racines que  $a_1, \dots, a_n$  dans  $\llbracket 0, p-1 \rrbracket$  (modulo  $p$ )

## A. Cas $m = 17$

1. Soit  $a \in \mathbb{Z}$ .

$$(17-a)^2 = 17^2 - 2 \times 17 \times a + a^2 = a^2 + 17(17+2a)$$

/1

Donc, en déduisant modulo 17, pour tout  $a \in \mathbb{Z}$ ,  $a^2 \equiv (17-a)^2[17]$ .

2. La question précédente nous signale la symétrie dans le calcul de  $a^2$ , modulo 17.

$a$	1	2	3	4	5	6	7	8
$17-a$	16	15	14	13	12	11	10	9
$a^2 = (17-a)^2$	1	4	9	16(= -1)	8	2	15(= -2)	13(= -4)

3. Un nombre est un résidu quadratique si et seulement si il est le carré d'un nombre  $a$ ; or on a fait la liste de tous les carrés possibles.

/1,5

Il y a exactement 8 résidus quadratiques modulo 17 : 1, 2, 4, 8, 9, 13, 15, 16  
 et modulo 17 :  $\sqrt{1} \in \{1, 16\}$ ,  $\sqrt{2} \in \{6, 11\}$ ,  $\sqrt{4} \in \{2, 15\}$ ,  $\sqrt{8} \in \{5, 12\}$ ,  
 $\sqrt{9} \in \{3, 14\}$ ,  $\sqrt{13} \in \{8, 9\}$ ,  $\sqrt{15} \in \{7, 10\}$  et  $\sqrt{16} \in \{4, 13\}$

4. C'est le petit théorème de Fermat :  $a^{p-1} \equiv 1[p]$ , avec  $p = 17$ , nombre premier

/1

pour tout  $a \in \llbracket 1, 16 \rrbracket$ ,  $a^{16} \% 17 = 1$ .

5. On peut (re)faire un tableau, cette fois-ci on ne regarde que les nombres de 1 à 8 car comme  $a^2 \equiv (17-a)^2[17]$ , en élevant à la puissance 4 :  $a^8 \equiv (17-a)^8[17]$ .

$a$	1	2	3	4	5	6	7	8
$a^2$	1	4	-7	-1	8	2	-2	-4
$a^4$	1	-1	-2	1	-4	4	4	-1
$a^8$	1	1	-1	1	-1	-1	-1	1

/2

$\{a \in \llbracket 1, 16 \rrbracket \mid a^8 \equiv 1[17]\} = \{1, 2, 4, 8, 9, 13, 15, 16\} = \{a^2[17], a \in \llbracket 1, 16 \rrbracket\}$

## B. Applications pseudo-indicatrices

1. Etude de  $\epsilon$  et  $\omega$ .

(a) Supposons que  $a$  est impair, un et seul cas suivant se produit :

- ou bien  $a \equiv 1[4]$ , alors  $4|a-1$ , donc  $\frac{a-1}{2}$  est pair et donc  $(-1)^{\frac{a-1}{2}} = 1 = \epsilon(a)$ .
- ou bien  $a \equiv 3[4]$ , alors  $4|a-3$ , donc  $\frac{a-3}{2} = \frac{a-1}{2} - 1$  est pair et  $\frac{a-1}{2} - 1$  est impair  
 ainsi  $(-1)^{\frac{a-1}{2}} = (-1) = \epsilon(a)$ .

/1

Puis, également, un et seul cas suivant se produit :

- ou bien  $a \equiv 1[8]$ , alors  $8|a-1$  donc  $\frac{a^2-1}{8} = \frac{a-1}{8}(a+1)$  est un pair car  $a+1$  est pair.  
 et donc  $(-1)^{\frac{a^2-1}{8}} = 1 = \omega(a)$ .
- ou bien  $a \equiv 7[8]$ , alors  $8|a+1$  donc  $\frac{a^2-1}{8} = \frac{a+1}{8}(a-1)$  est un pair car  $a-1$  est pair.  
 et donc  $(-1)^{\frac{a^2-1}{8}} = 1 = \omega(a)$ .
- ou bien  $a \equiv 3[8]$ , alors  $a = 8k+3$ , donc  $a^2-1 = 8(8k^2+6k)+9-1 = 8(2(4k^2+3k)+1)$   
 donc  $\frac{a^2-1}{8} = 2(4k^2+3k)+1$  est un nombre impair et donc  $(-1)^{\frac{a^2-1}{8}} = -1 = \omega(a)$ .
- ou bien  $a \equiv 5[8]$ , alors  $a = 8k+5$ , donc  $a^2-1 = 8(8k^2+10k)+25-1 = 8(2(4k^2+5k+1)+1)$   
 donc  $\frac{a^2-1}{8} = 2(4k^2+5k+1)+1$  est un nombre impair et donc  $(-1)^{\frac{a^2-1}{8}} = -1 = \omega(a)$ .

/1,5

Donc pour tout entier  $a$  impair,  $\epsilon(a) = (-1)^{\frac{a-1}{2}}$  et  $\omega(a) = (-1)^{\frac{a^2-1}{8}}$ .

(b) Si  $a$  ou  $a'$  est pair, alors  $\epsilon(a) = 0$  ou  $\epsilon(a') = 0$ , d'où  $\epsilon(a)\epsilon(a') = 0$

Et par ailleurs,  $aa'$  est alors pair donc  $\epsilon(aa') = 0$ . Donc  $\epsilon(aa') = \epsilon(a)\epsilon(a')$

On a de même  $\omega(aa') = 0 = \omega(a)\omega(a')$ .

/1

Si  $a$  et  $a'$  sont impair, alors  $aa'$  aussi :

$$\epsilon(aa') = (-1)^{\frac{aa'-1}{2}} = (-1)^{\frac{aa'-1}{2}} \text{ et } \epsilon(a)\epsilon(a') = (-1)^{\frac{a-1}{2}}(-1)^{\frac{a'-1}{2}} = (-1)^{\frac{a+a'-2}{2}}.$$

Or  $\frac{a+a'-2}{2} - \frac{aa'-1}{2} = \frac{a+a'-aa'-1}{2} = \frac{-(a-1)(a'-1)}{2}$  est un nombre pair ( $a$  et  $a'$  impaires).

Donc  $\frac{a+a'-2}{2}$  et  $\frac{aa'-1}{2}$  ont même parité et donc  $\epsilon(aa') = \epsilon(a)\epsilon(a')$

De même on étudie la parité de  $\frac{(a^2-1)+(a'^2-1)-(aa')^2-1}{8} = \frac{a^2+a'^2-aa')^2-1}{8} = \frac{-(a^2-1)(a'^2-1)}{8}$

Or  $4|a^2-1$ , car  $a = 2k+1$  est impair donc  $a^2-1 = 4(k^2+k)$ . De même  $4|a'^2-1$ , donc  $16|(a^2-1)(a'^2-1)$ .

Et donc  $\frac{(a^2-1)+(a'^2-1)}{8}$  et  $\frac{(aa')^2-1}{8}$  ont même parité :  $\omega(aa') = \omega(a)\omega(a')$

/1,5

Pour tout  $a, a' \in \mathbb{Z}$ ,  $\epsilon(aa') = \epsilon(a)\epsilon(a')$  et  $\omega(aa') = \omega(a)\omega(a')$ .

2. Etude de la fonction  $\theta$ .

(a) Comme  $2|2$ ,  $\theta(1, 2) = 0$ .

Comme  $1 \equiv 1[4]$  et  $3$  n'est pas divisible par  $2$  :  $\theta(1, 3) = 1$ .

Comme  $5 \equiv 1[4]$  et  $9$  n'est pas divisible par  $2$  :  $\theta(5, 9) = 1$ .

/1,5

$$\theta(1, 3) = 1 = \theta(5, 9) \quad \theta(1, 2) = 0$$

(b) La définition de  $\theta$  est parfaitement symétrique en  $a$  et  $a'$ .

/1

$$\forall a, a' \in \mathbb{Z}, \theta(a, a') = \theta(a', a)$$

(c) On suppose que  $a$  et  $a'$  sont des entiers impairs.

Un et seul cas se produit :

- $a \equiv 3[4]$  et  $a' \equiv 3[4]$ , alors il existe  $k, k' \in \mathbb{Z}$  tels que  $a = 4k + 3$  et  $a' = 4k' + 3$ .

$$\text{Donc } \frac{(a-1)(a'-1)}{4} = \frac{(4k-2)(4k'-2)}{4} = (4kk' - 2k' - 2k + 1), \text{ impair.}$$

$$\text{Dans ce cas : } (-1)^{\frac{(a-1)(a'-1)}{4}} = -1 = \theta(a, a').$$

- $a \equiv 1[4]$  ou  $a' \equiv 1[4]$ . Par symétrie de  $\theta(a, a')$ , il suffit d'étudier un cas, sans perte de généralité.

$$\text{On suppose donc que } a = 4k + 1, \text{ donc } \frac{(a-1)(a'-1)}{4} = k(a' - 1), \text{ pair car } a \text{ est impair.}$$

$$\text{Dans ce cas : } (-1)^{\frac{(a-1)(a'-1)}{4}} = 1 = \theta(a, a'). \quad /2$$

$$\boxed{\text{Dans le cas où } a \text{ et } a' \text{ sont des entiers impairs, } \theta(a, a') = (-1)^{\frac{(a-1)(a'-1)}{4}}.}$$

(d) Soient  $a, b, a' \in \mathbb{Z}$ ,

- Si  $a$  ou  $b$  est pair,  $ab$  l'est également et donc  $\theta(ab, a') = 0 = \theta(a, a') \times \theta(b, a')$ .
- Si  $a'$  est pair alors  $\theta(ab, a') = 0 = \theta(a, a')\theta(b, a')$ .
- Il reste le cas où  $a, b$  et  $a'$  sont impairs.

Comme précédemment, on étudie simplement la parité de

$$\begin{aligned} \frac{(ab-1)(a'-1)}{4} - \frac{(a-1)(a'-1)}{4} - \frac{(b-1)(a'-1)}{4} &= \frac{aba' - a' - ab + 1 - aa' + a + a' - 1 - ba' + b + a' - 1}{4} \\ &= \frac{aba' - ab - aa' - ba' + a + b + a' - 1}{4} = \frac{(a-1)(b-1)(a'-1)}{4} \end{aligned}$$

Or  $a-1, b-1$  et  $a'-1$  sont divisibles par 2, donc (produit)  $8|(a-1)(b-1)(a'-1)$ .

Ainsi  $\frac{(ab-1)(a'-1)}{4} - \frac{(a-1)(a'-1)}{4} - \frac{(b-1)(a'-1)}{4}$  est pair.

$$\text{Donc } \theta(ab, a') = \theta(a, a') \times \theta(b, a') \quad /2,5$$

$$\boxed{\text{Pour tout } a, b, a' \in \mathbb{Z}, \theta(ab, a') = \theta(a, a') \times \theta(b, a').}$$

## C. Symbole de Legendre

1. Si  $a \equiv a'[m]$  et  $b \equiv b'[m]$ .

alors  $m|(a-a'), m|(b-b')$  Donc  $m$  divise  $ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + b'(a-a')$ , par stabilité de divisibilité sur les combinaisons linéaires.

Donc par indépendance du représentant, on peut affirmer : /1

$$\boxed{\text{pour tout } a, b \in \frac{\mathbb{Z}}{m\mathbb{Z}}, \overbrace{ab}^{\cdot} = \dot{a} \times \dot{b}.}$$

2. On raisonne directement par équivalence :

$$\begin{aligned} \dot{r} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* &\iff \exists \dot{s} \in \frac{\mathbb{Z}}{m\mathbb{Z}} \text{ tel que } \dot{s}\dot{r} = \dot{r}\dot{s} = \dot{1} &\iff \exists s \in \mathbb{Z} \text{ tel que } sr(\equiv rs) \equiv 1[m] \\ &\iff \exists s \in \mathbb{Z}, k \in \mathbb{Z} \text{ tels que } sr = 1 + km &\iff \exists s \in \mathbb{Z}, k' \in \mathbb{Z} \text{ tels que } sr + k'm = 1 \\ &\iff r \wedge m = 1 \end{aligned}$$

d'après l'identité de BÉZOUT /2

$$\boxed{\dot{r} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \text{ si et seulement si } r \wedge m = 1.}$$

3. Dans le cas où  $m = p$  est premier, tout les nombres de 1 à  $p-1$  sont premiers avec  $p$ , /1

$$\boxed{\text{Donc } \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* = \{\dot{1}, \dot{2}, \dots, \dot{p-1}\}}$$

4. Deux morphismes de groupes multiplicatifs

(a) Pour tout  $ab \in \mathbb{F}_p$  (on fait la confusion entre  $a$  et  $\dot{a}$ ) :

$$\psi_p(ab) = \overbrace{(ab)}^{\cdot} \times \overbrace{(ab)}^{\cdot} \underset{\text{d'après 1}}{=} \overbrace{(ab)^2}^{\cdot} \underset{\text{commutativité dans } \mathbb{Z}}{=} \overbrace{a^2 b^2}^{\cdot} \underset{\text{d'après 1}}{=} \overbrace{a^2}^{\cdot} \times \overbrace{b^2}^{\cdot} = \varphi_p(a)\varphi_p(b)$$

$$\boxed{\psi_p \text{ est donc un morphisme de groupes}} \quad /2$$

- (b) Soit  $\dot{x} \in \mathbb{F}_p$ ,  $\psi_p \circ \varphi_p(\dot{x}) = (\dot{x})^{p-1} = \overbrace{x^{p-1}} = \dot{1}$ ,  
car d'après le petit théorème de Fermat, pour tout  $x$  tel que  $x \wedge p = 1$ , on a  $x^{p-1} \equiv 1[p]$ . /2

$$\boxed{\psi_p \circ \varphi_p = \mathbf{1}_{\mathbb{F}_p}}$$

- (c) Soit  $\dot{x} \in \text{Ker } \psi_p$ , i.e.  $x^2 \equiv 1[p]$ .  
Donc  $p|x^2 - 1 = (x-1)(x+1)$ .  
Or  $p$  est un nombre premier donc  $p|x-1$  ou  $p|x+1$   
Ainsi  $x \equiv 1[p]$  ou  $x \equiv -1[p]$ , i.e.  $x \equiv p-1[p]$ .  
Réciproquement, si  $x = 1$ , alors  $\psi_p(\dot{x}) = \dot{1}^2 = \dot{1}^2 = \dot{1}$  et si  $x = -p1$ ,  $\psi_p(\dot{x}) = (-\dot{1})^2 = \dot{1}$ .  
Par double inclusion : /1,5

$$\boxed{\text{Ker } \psi_p = \{\dot{1}, \overbrace{p-1}\}}$$

- (d) Soit  $\dot{x} \in \text{Im } \varphi_p$ .  
Donc il existe  $\dot{a} \in \mathbb{F}_p$  tel que  $\varphi_p(\dot{a}) = \dot{x}$ .  
On a alors  $\psi_p(\dot{x}) = (\psi_p \circ \varphi_p)(\dot{a}) = \mathbf{1}_{\mathbb{F}_p}(\dot{a}) = 1$ .  
Ainsi,  $\dot{x} \in \text{Ker } \psi_p$ . /1,5

$$\boxed{\text{Im } \varphi_p \subset \text{Ker } \psi_p = \{\dot{1}, \overbrace{p-1}\}}$$

- (e) On sait que  $\text{Im } \varphi_p = \{\dot{1}, \overbrace{p-1}\}$ .  
Donc  $\mathbb{F}_p^* = \{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} \cup \{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$ . Cette réunion est disjointe.  
En prenant les cardinaux :  $p-1 = \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} + \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$ .  
Puis le polynôme  $t_1 : x \mapsto x^{\frac{p-1}{2}} - 1$  admet au plus  $\frac{p-1}{2}$  racines distinctes dans  $\llbracket 1, p-1 \rrbracket$   
(0 n'est pas racine).  
Or  $h \in \{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} \iff t_1(h) = 0$ . Donc  $\text{card}(\varphi_p^{-1}(\{\dot{1}\})) \leq \frac{p-1}{2}$ .  
De même, le polynôme  $t_2 : x \mapsto x^{\frac{p-1}{2}} + 1$  admet au plus  $\frac{p-1}{2}$  racines distinctes dans  $\llbracket 1, p-1 \rrbracket$   
(0 n'est pas racine).  
 $h \in \{k \in \mathbb{F}_p \mid \varphi_p(k) \equiv -1 \equiv p-1[p]\} \iff t_2(h) = 0 : \text{card}(\varphi_p^{-1}(\{\overbrace{p-1}\})) \leq \frac{p-1}{2}$ .  
Pour que la somme  $\text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = 1\} + \text{card}\{k \in \mathbb{F}_p \mid \varphi_p(k) = -1\}$  donne  $p-1$ ,  
il faut et il suffit que /3

$$\boxed{\text{card}(\varphi_p^{-1}(\{\dot{1}\})) = \text{card}(\varphi_p^{-1}(\{\overbrace{p-1}\})) = \frac{p-1}{2}}$$

- (f)  $\varphi_p(-1) = 1 \iff (-1)^{\frac{p-1}{2}} \equiv 1[p]$ .  
Si  $p \equiv 1[4]$ , alors  $\frac{p-1}{2}$  est un nombre pair et  $(-1)^{\frac{p-1}{2}} = 1$ , donc  $(-1)^{\frac{p-1}{2}} \equiv 1[p]$ .  
Si  $p \equiv 3[4]$ , alors  $\frac{p-1}{2}$  est un nombre impair et  $(-1)^{\frac{p-1}{2}} = -1$ , donc  $(-1)^{\frac{p-1}{2}} \equiv -1[p]$ . /1

$$\boxed{\varphi_p(-1) = 1 \iff p \equiv 1[4]}$$

## 5. Symbole de LEGENDRE.

- (a) Supposons que  $a \equiv a'[p]$ .  
• Si  $p|a$  alors  $p|a'$  et donc  $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right) = 0$   
• Si  $\left(\frac{a}{p}\right) = 1$ , alors  $a \wedge p = 1$  et donc  $a' \wedge p = 1$ .  
Et il existe  $b \in \mathbb{Z}$  tel que  $a \equiv b^2[p]$  et donc  $a' \equiv b^2[p]$  et donc  $\left(\frac{a'}{p}\right) = 1 = \left(\frac{a}{p}\right)$   
• Si  $\left(\frac{a}{p}\right) = -1$ , alors  $a \wedge p = 1$  et donc  $a' \wedge p = 1$ .  
Et  $\forall b \in \mathbb{Z}$  tel que  $a \not\equiv b^2[p]$  et donc  $a' \not\equiv b^2[p]$  et donc  $\left(\frac{a'}{p}\right) = -1 = \left(\frac{a}{p}\right)$  /2

$$\boxed{\text{Si } a \equiv a'[p], \text{ alors } \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)}$$

- (b) Les résidu quadratique modulo 17 sont 1, 2, 4, 8, 9, 13, 15, 16 et leur congruence modulo 17.  
Or  $30 \equiv 13[17]$ ,  $32 \equiv 15[17]$ ,  $33 \equiv 16[17]$ ,  $35 \equiv 1[17]$ ,  $36 \equiv 2[17]$ ,  $38 \equiv 4[17]$ .  
On a donc la liste suivante : /1

$a$	30	31	32	33	34	35	36	37	38	39	40
$\left(\frac{a}{17}\right)$	1	-1	1	1	0	1	1	-1	1	-1	-1

- (c) Il suffit de se concentrer sur les nombres de  $\{0, 1, 2\}$ , on exploitera ensuite la congruence.
- si  $a \equiv 0[3]$ , alors  $\left(\frac{a}{3}\right) = 0 \equiv a[3]$
  - si  $a \equiv 1[3]$ , alors  $a = 1^2$ , donc  $\left(\frac{a}{3}\right) = 1 \equiv a[3]$
  - si  $a \equiv 2[3]$ , alors comme  $1^2 \equiv 2^2 = 1[3]$ , 2 n'est pas un résidu quadratique, donc  $\left(\frac{a}{3}\right) = -1 \equiv 2 \equiv a[3]$

/1,5

$$\boxed{\text{Pour tout } a \in \mathbb{Z}, \left(\frac{a}{3}\right) \equiv a[3].}$$

- (d) Soit  $a \in \mathbb{Z}$ , on sait d'après la question 5.(a) que  $\left(\frac{a}{p}\right) = \left(\frac{a \% p}{p}\right)$ .

- Si  $p|a$ , alors  $a \% p = 0$  et donc  $\left(\frac{a}{p}\right) = 0 = \varphi_p(a \% p)$ .
- Si  $p \wedge a = 1$ , alors  $a \% p \in \mathbb{N}_{p-1}$ .

Si  $a$  est un résidu quadratique, il existe  $b \in \mathbb{N}_{p-1}$  tel que  $a = b^2$ , donc  $x^2 - a$  se factorise en  $(x - b)(x + b)$  modulo  $p$  (cf. préliminaires).

Ainsi,  $a$  admet exactement deux racines carrées modulo  $p$ .

Par conséquent, il y a deux options :

- ou bien  $x^2 - a$  admet deux racines l'une entre 1 et  $\frac{p-1}{2}$  et l'autre entre  $\frac{p+1}{2}$  et  $p-1$ ,
- ou bien  $x^2 - a$  n'admet aucune racine.

$$\text{card}\{(x^2) \% p; x \in \mathbb{Z}\} = \text{card}\{(x^2) \% p, x \in \llbracket 1, \frac{p-1}{2} \rrbracket\} = \frac{p-1}{2}$$

Par ailleurs,

si  $a$  est un résidu quadratique, alors il existe  $b \in \mathbb{Z}$  tel que  $a \% p \equiv b^2[p]$  et donc  $\varphi_p(a \% p) = \varphi_p(\psi_p(b)) = 1$

ainsi  $a \in \text{Ker } \varphi_p = \{x \in \mathbb{F}_p \mid \varphi_p(x) = 1\}$ .

On a donc l'inclusion :  $\{(x^2) \% p; x \in \mathbb{Z}\} \subset \text{Ker } \varphi_p$ .

Or on a démontré que  $\text{card}\{(x^2) \% p; x \in \mathbb{Z}\} = \frac{p-1}{2}$  et en 4.(e) :  $\text{card}\varphi_p^{-1}(\{1\}) = \frac{p-1}{2}$ .

Ainsi, on a exactement l'égalité des ensembles (inclusion + égalité des cardinaux) :

$$\{(x^2) \% p; x \in \mathbb{Z}\} = \varphi_p^{-1}(\{1\})$$

Et par passage au complémentaire :

$$\varphi_p^{-1}(\{-1\}) = \{a \in \mathbb{F}_p, a \text{ non résidu quadratique}\}$$

/3

$$\boxed{\forall a \in \mathbb{Z}, \left(\frac{a}{p}\right) = \varphi_p(a \% p)}$$

- (e) On exploite le fait que  $\varphi_p$  est un morphisme de groupe (pour  $a$  et  $a'$  non divisible par  $p$ ).

Si  $p$  divise  $a$  ou  $a'$ , donc l'un des termes est nul :  $\left(\frac{a}{p}\right) \left(\frac{a'}{p}\right)$

alors que  $p$  divise  $aa'$  donc  $\left(\frac{aa'}{p}\right) = 0$

Si  $p$  ne divise ni  $a$  ni  $a'$  :

$$\left(\frac{aa'}{p}\right) = \varphi_p((aa') \% p) = \varphi_p((a \% p) \times (a' \% p)) = \varphi_p(a \% p) \varphi_p(a' \% p) = \left(\frac{a}{p}\right) \left(\frac{a'}{p}\right)$$

/1,5

$$\boxed{\forall a, a' \in \mathbb{Z}, \left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{a'}{p}\right)}$$

- (f) Supposons que  $a \wedge p = 1$ . On applique la propriété précédente, et comme  $a^2$  est un carré :

/1

$$\boxed{\left(\frac{a^2 a'}{p}\right) = \left(\frac{a^2}{p}\right) \left(\frac{a'}{p}\right) = 1 \left(\frac{a'}{p}\right)}$$

6. D'après 4.(e), il y a autant de racines quadratiques que de non racines quadratiques :  $\frac{p-1}{2}$ ,

/2

$$\boxed{\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \frac{p-1}{2} \times 1 + \frac{p-1}{2} \times (-1) = 0}$$

## D. Somme de Gauss et réciprocity quadratique

### 1. Somme de GAUSS.

On fixe un nombre premier  $p > 2$  et considère  $\xi = e^{2i\pi/p}$  et  $\tau = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k$ .

(a) Il s'agit d'une somme de  $p$  termes consécutifs d'une suite géométrique de raison  $\xi \neq 1$ . /1,5

$$\boxed{\sum_{k=0}^{p-1} \xi^k = \frac{1 - \xi^p}{1 - \xi} = \frac{1 - e^{2i\pi}}{1 - \xi} = 0}$$

(b) On note  $h_k : s \mapsto ks$ .

Comme  $p$  est premier,  $k$  est inversible modulo  $p$  (dans  $\mathbb{F}_p$ ).

On note  $k'$  tel que  $kk' \equiv 1[p]$  (BÉZOUT).

On a alors  $h_k \circ h_{k'}(s) = kk's = s = k'ks = h_{k'} \circ h_k(s)$ . /1,5

Donc  $h_k$  est bijective.

Puis, les sommes peuvent commencer à 1 car  $\left(\frac{0}{p}\right) = 0$

$$\tau^2 = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \xi^k \times \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) \xi^s = \sum_{k=1}^{p-1} \sum_{h=1}^{p-1} \left(\frac{kh}{p}\right) \xi^{k+h}$$

Puis on fait le changement de variable :  $h = h_k(s) = ks$  avec  $h_k$  bijective (de la variable  $h$  à la variable  $s$ ) : /1,5

$$\tau^2 = \sum_{k=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{k^2s}{p}\right) \xi^{k+ks} = \sum_{s=1}^{p-1} \sum_{k=1}^{p-1} \left(\frac{s}{p}\right) \xi^{k+ks}$$

puisque'on a vu que  $\left(\frac{k^2s}{p}\right) = \left(\frac{s}{p}\right)$ . Donc

$$\tau^2 = \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \sum_{k=1}^{p-1} (\xi^{1+s})^k$$

Comme : si  $1 + s \neq 0$ ,  $\sum_{k=1}^{p-1} (\xi^{1+s})^k = \sum_{k=0}^{p-1} (\xi^{1+s})^k - 1 = \frac{(\xi^{1+s})^p - 1}{\xi^{1+s} - 1} - 1 = -1$ .

et si  $1 + s = 0$ ,  $\sum_{k=1}^{p-1} (\xi^{1+s})^k = \sum_{k=1}^{p-1} 1 = p - 1$ , On trouve donc :

$$\tau^2 = \left(\frac{1}{p}\right) (p - 1) - \sum_{s=2}^{p-1} \left(\frac{s}{p}\right)$$

Or, on a vu en fin de partie précédente que  $\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) = 0$ , donc  $\sum_{s=2}^{p-1} \left(\frac{s}{p}\right) = -\left(\frac{1}{p}\right)$ , /2,5

$$\boxed{\tau^2 = \left(\frac{1}{p}\right) p = \epsilon(p)p}$$

(c) On considère  $q$ , un nombre premier impair et distinct de  $p$ .

Pour tout entier  $k \in \llbracket 1, q - 1 \rrbracket$ ,  $\binom{q}{k} = q \times (q - 1)(q - 2) \dots (q - k + 1)k! \in \mathbb{Z}$

Donc  $q$  divise  $k! \times \binom{q}{k}$ .

Or pour tout  $i \in \llbracket 1, k \rrbracket$ ,  $i \wedge q = 1$ , donc d'après le lemme de Gauss : /1

$$\boxed{\forall k \in \llbracket 1, q - 1 \rrbracket, q \mid \binom{q}{k}}$$

On démontre alors le résultat demandé par récurrence :

$$\left(\sum_{i=0}^s a_i\right)^q = \left(\underbrace{\sum_{i=0}^{s-1} a_i}_{=A} + a_s\right)^q = \sum_{k=0}^q \binom{q}{k} A^k a_s^{q-k}$$

Or  $q \mid \binom{k}{q}$ , donc en plongeant modulo  $q$  :

$$\left( \sum_{i=0}^s a_i \right)^q \equiv A^0 a_s^{q-0} + A^q a_s^0 \equiv a_s^q + A^q \pmod{q}$$

Puis, on applique le résultat à l'ordre  $s-1$  pour calculer  $A^q$  :

/2

$$\boxed{\left( \sum_{i=0}^s a_i \right)^q = \sum_{i=0}^s a_i^q \pmod{q}}$$

(d) Avec le résultat précédent, on trouve (modulo  $q$ ) :

$$\tau^q = \left( \sum_{k=1}^{p-1} a_k \right)^q \equiv \sum_{k=1}^{p-1} a_k^q \equiv \sum_{k=1}^{p-1} \left( \frac{k}{p} \right)^q \xi^{qk} \pmod{q}$$

Puis, comme  $q$  est un nombre impair et que  $\left( \frac{k}{p} \right) = \pm 1$ , on a  $\left( \frac{k}{p} \right)^q = \left( \frac{k}{p} \right)$ .

/1,5

$$\boxed{\left( \frac{q}{p} \right) \tau^q \equiv \sum_{k=1}^{p-1} \left( \frac{q}{p} \right) \left( \frac{k}{p} \right) \xi^{qk} \equiv \sum_{s=1}^{p-1} \left( \frac{s}{p} \right) \xi^s \equiv \tau \pmod{q}}$$

En exploitant toujours le changement de variable  $k \rightarrow s$  avec  $s = kq$ .

(e) Par ailleurs

$$\tau^{q-1} = (\tau^2)^{\frac{q-1}{2}} = (\epsilon(p)p)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}}$$

Or  $p^{\frac{q-1}{2}}$  ressemble au calcul du symbole de LEGENDRE :

$$p^{\frac{q-1}{2}} \equiv \left( \frac{p}{q} \right) \pmod{q}$$

/1,5

$$\boxed{\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left( \frac{p}{q} \right) \pmod{q}}$$

## 2. Réciprocité quadratique.

(a) Comme  $\tau$  n'est pas nul, il est inversible dans  $\mathbb{F}_q$ , on a donc deux résultats concernant  $\tau^{q-1}$  :

$$\tau^{q-1} \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left( \frac{p}{q} \right) \equiv \left( \frac{q}{p} \right)^{-1} = \left( \frac{q}{p} \right) \pmod{q}$$

On a  $\left( \frac{q}{p} \right)^{-1} = \left( \frac{q}{p} \right)$ , car il s'agit d'un élément de  $\{-1, 1\}$ .

Enfin, ces deux nombres congruents modulo  $q$  sont deux nombres de  $\{-1, 1\}$ , donc leur équivalence modulo  $q$  signifie leur égalité.

/2

$$\boxed{\text{Pour } p \text{ et } q \text{ deux nombres premiers impairs distincts, } \left( \frac{p}{q} \right) = (-1)^{(p-1)(q-1)/4} \left( \frac{q}{p} \right)}$$

(b) Il s'agit de calculer le symbole de LEGENDRE  $\left( \frac{17}{41} \right)$  en exploitant la réciprocité quadratique :

$$\left( \frac{17}{41} \right) = (-1)^{16 \times 40/4} \left( \frac{41}{17} \right) = 1 \left( \frac{7}{17} \right) = -1$$

car  $41 \equiv 7[17]$ , et puisqu'on sait que 7 n'est pas un résidu quadratique modulo 17.

/2

$$\boxed{17 \text{ n'est pas un carré de } \frac{\mathbb{Z}}{41\mathbb{Z}}}$$

## E. Symbole de Jacobi et réciprocité quadratique généralisée

### 1. Symbole de JACOBI.

(a) Soient  $a, a' \in \mathbb{Z}$ ,  $m, m' \geq 3$ , impairs tels que  $m \wedge m' = 1$ .

Supposons que  $m = \prod_{i=1}^s p_i^{\alpha_i}$  et  $m' = \prod_{j=1}^r p'_j{}^{\beta_j}$ .

Comme  $m \wedge m' = 1$ , alors pour tout  $i \in \mathbb{N}_s$  et  $j \in \mathbb{N}_r$ ,  $p_i \neq p'_j$ .

On a alors

$$\left(\frac{aa'}{m}\right) = \prod_{i=1}^s \left(\frac{aa'}{p_i}\right)^{\alpha_i} = \prod_{i=1}^s \left(\frac{a}{p_i}\right)^{\alpha_i} \prod_{i=1}^s \left(\frac{a'}{p_i}\right)^{\alpha_i} = \left(\frac{a}{m}\right) \left(\frac{a'}{m}\right)$$

par multiplicativité du symbole de LEGENDRE.

Puis :

$$\left(\frac{a}{mm'}\right) = \left(\frac{a}{\prod_{i=1}^s p_i^{\alpha_i} \prod_{j=1}^r p'_j{}^{\beta_j}}\right) = \prod_{i=1}^s \left(\frac{a}{p_i}\right)^{\alpha_i} \prod_{j=1}^r \left(\frac{a}{p'_j}\right)^{\beta_j} = \left(\frac{a}{m}\right) \left(\frac{a}{m'}\right)$$

/3

$$\boxed{\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{a'}{m}\right) \quad \text{et} \quad \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{m'}\right)}$$

(b)  $51 = 3 \times 17$  :

$$\left(\frac{14}{51}\right) = \left(\frac{14}{3}\right) \left(\frac{14}{17}\right) = \left(\frac{-1}{3}\right) \left(\frac{-3}{17}\right) = -1 \times -1 = 1$$

/2

$$\boxed{\left(\frac{14}{51}\right) = 1}$$

### 2. Loi de réciprocité.

Soient  $n, m \in \mathbb{Z}$ , impairs, positifs et premiers entre eux.

- si  $n \wedge m \neq 1$ , alors il existe un facteur premier commun noté  $p$  à  $n$  et  $m$ .

Dans ce cas, dans la décomposition  $\prod_{p|n, p \in \mathcal{P}} \left(\frac{m}{p}\right)^{v_p(n)}$  se trouve un facteur nul.

De même pour  $\prod_{p|m, p \in \mathcal{P}} \left(\frac{n}{p}\right)^{v_p(m)}$ .

Et donc  $\left(\frac{m}{n}\right) = 0 = \left(\frac{n}{m}\right)$ .

- Supposons que  $m = \prod_{i=1}^s p_i^{\alpha_i}$  et  $n = \prod_{j=1}^r p'_j{}^{\beta_j}$  avec  $m \wedge n = 1$ ,

donc pour tout  $i \in \mathbb{N}_s$  et  $j \in \mathbb{N}_r$  :  $p_i \neq p'_j$ .

Par multiplativité, et comme  $(-1)^{\frac{(p_i-1)(p'_j-1)}{4}} = \theta(p_i, p'_j)$  :

$$\begin{aligned} \left(\frac{n}{m}\right) &= \prod_{i=1}^s \prod_{j=1}^r \left(\frac{p'_j}{p_i}\right)^{\alpha_i \beta_j} = \prod_{i=1}^s \prod_{j=1}^r \left[ (-1)^{\frac{(p_i-1)(p'_j-1)}{4}} \left(\frac{p_i}{p'_j}\right) \right]^{\alpha_i \beta_j} = \prod_{i=1}^s \prod_{j=1}^r \left[ \theta(p_i, p'_j) \left(\frac{p_i}{p'_j}\right) \right]^{\alpha_i \beta_j} \\ &= \prod_{i=1}^s \left( \prod_{j=1}^r \theta(p_i, p'_j)^{\alpha_i \beta_j} \right) \times \prod_{i=1}^s \left( \prod_{j=1}^r \left(\frac{p_i}{p'_j}\right)^{\alpha_i \beta_j} \right) = \prod_{i=1}^s \theta(p_i, \prod_{j=1}^r p'_j{}^{\beta_j})^{\alpha_i} \times \left(\frac{m}{n}\right) \\ &= \prod_{i=1}^s \theta(p_i, n)^{\alpha_i} \times \left(\frac{m}{n}\right) = \theta(m, n) \left(\frac{m}{n}\right) \end{aligned}$$

Comme  $\theta(m, n) = \theta(m, n)^{-1}$  :

/3

$$\boxed{\left(\frac{m}{n}\right) = \theta(m, n) \left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right)}$$

### 3. Lois complémentaires.

Soit  $n$  un entier impair, on utilise les définitions et les propriétés multiplicatives de  $\epsilon$  et  $\omega$  :

$$\left(\frac{-1}{n}\right) = \prod_{j=1}^r \left(\frac{-1}{p'_j}\right)^{\beta_j} = \prod_{j=1}^r \epsilon(p_j)^{\beta_j} = \epsilon \left( \prod_{j=1}^r p'_j{}^{\beta_j} \right) = \epsilon(n)$$

Et

$$\binom{2}{n} = \prod_{j=1}^r \binom{2}{p'_j}^{\beta_j} = \prod_{j=1}^r \omega(p_j)^{\beta_j} = \omega\left(\prod_{j=1}^r p_j^{\beta_j}\right) = \omega(n)$$

Puis par expression analytique de  $\epsilon$  et  $\omega$  :

/2

Pour tout $n$ entier impair positif : $\binom{-1}{n} = \epsilon(n) = (-1)^{\frac{n-1}{2}}$ et $\binom{2}{n} = \omega(n) = (-1)^{\frac{n^2-1}{8}}$
---