DM 16 : un corrigé.

Partie I

1.a) Supposons que l'équation (E) : $\xi^2 = \overline{a}$ possède au moins une solution, notée $\xi_0 \in \mathbb{Z}/p\mathbb{Z}$. Alors $(E) \iff \xi^2 - \xi_0^2 = 0 \iff (\xi - \xi_0)(\xi + \xi_0) = 0$, or $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier, donc c'est en particulier un anneau intègre.
Ainsi, $(E) \iff [\xi = \xi_0$ ou $\xi = -\xi_0]$.
De plus, $\xi_0 = -\xi_0 \Rightarrow \overline{2}\xi_0 = 0 \Rightarrow \xi_0 = 0$, car $p \geq 3$, donc $\overline{2} \neq 0$.
Ainsi, $\xi_0 = -\xi_0 \Rightarrow \overline{a} = 0 \Rightarrow p|a$, ce qui est faux.
Ainsi ξ_0 et $-\xi_0$ sont les deux seules racines distinctes de (E), lorsque (E) possède au moins une solution. On a bien montré que (E) possède exactement 0 ou 2 solutions.

1.b) Notons R l'ensemble des résidus quadratiques et notons f : $\mathbb{Z}/p\mathbb{Z}^* \longrightarrow R$ l'application définie par $f(x) = x^2$. f est surjective par définition de R et d'après la question précédente, pour tout $\alpha \in R$, le cardinal de $f^{-1}(\{\alpha\})$ est égal à 2, donc d'après le principe des bergers, $|\mathbb{Z}/p\mathbb{Z}^*| = 2|R|$. Ainsi, $|R| = \dfrac{p-1}{2}$.
Il y a donc $\frac{p-1}{2}$ résidus quadratiques et $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ non-résidus quadratiques.

1.c) Dans $\mathbb{Z}/11\mathbb{Z}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{9}$, $\overline{4}^2 = \overline{5}$, $\overline{5}^2 = \overline{3}$,
puis $\overline{6}^2 = (-\overline{5})^2 = \overline{3}$, $\overline{7}^2 = (-\overline{4})^2 = \overline{5}$ etc.
On en déduit que les RQ modulo 11 sont 1, 3, 4, 5 et 9 et que les NRQ modulo 11 sont 2, 6, 7, 8, et 10.

1.d.α) Soit $a \in \mathbb{Z}$ tel que p ne divise pas a.
L'application f de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ dans $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ définie par $f(\overline{k}) = \overline{ka}$ est une bijection : en effet, p est premier et p ne divise pas a, donc $\overline{a} \neq 0$, donc $\overline{a}$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$. Ainsi f est correctement définie, bijective d'application réciproque $\overline{k} \longmapsto \overline{a}^{-1}\overline{k}$.
On en déduit que, pour tout $k \in \{1, \ldots, p-1\}$, $\left(\dfrac{ka}{p}\right)$ est défini,

et que $\displaystyle\sum_{k=1}^{p-1}\left(\frac{ka}{p}\right) = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \frac{p-1}{2} - \frac{p-1}{2} = 0$, d'après la question précédente.

1.d.β.1)
$\diamond$ Supposons que $k' = p-1$. Alors $\overline{k} = \overline{k'}^{-1} = \overline{-1}^{-1} = \overline{-1} = \overline{p-1}$, ce qui est faux car $k \in \{1, \ldots, p-2\}$. Ainsi $k' \neq p-1$.

$\diamond$ On remarque que p ne divise ni k, ni $k'+1$, ni $k+1$, donc p étant premier, p ne divise pas $k(k+1)$ ni $k'+1$, donc les symboles $\Big(\dfrac{k(k+1)}{p}\Big)$ et $\Big(\dfrac{k'+1}{p}\Big)$ sont bien définis.

Supposons que $\Big(\dfrac{k(k+1)}{p}\Big) = 1$. Il existe $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ tel que $\overline{k(k+1)} = x^2$. Alors $(\overline{k'}x)^2 = \overline{k'k} \times \overline{k'(k+1)} = \overline{1+k'}$, donc $\Big(\dfrac{k'+1}{p}\Big) = 1$.

Réciproquement, supposons que $\Big(\dfrac{k'+1}{p}\Big) = 1$. Il existe $y \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ tel que $\overline{k'+1} = y^2$. Alors $(\overline{k}y)^2 = \overline{k}^2 \times (\overline{k}^{\,-1} + 1) = \overline{k+k^2} = \overline{k(k+1)}$, donc $\Big(\dfrac{k(k+1)}{p}\Big) = 1$.

Ceci démontre que $\Big(\dfrac{k(k+1)}{p}\Big) = \Big(\dfrac{k'+1}{p}\Big)$.

1.d.β.2) D'après la question précédente, $\displaystyle\sum_{k=1}^{p-2}\Big(\frac{k(k+1)}{p}\Big) = \sum_{k=1}^{p-2}\Big(\frac{\overline{k}^{\,-1}+1}{p}\Big)$, en convenant que $\Big(\dfrac{\overline{a}}{p}\Big) = \Big(\dfrac{a}{p}\Big)$. Mais l'application $x \longmapsto x^{-1}$ est une bijection involutive de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ dans lui-même, et $\overline{p-1}^{\,-1} = \overline{-1}^{\,-1} = \overline{-1} = \overline{p-1}$,

donc $\displaystyle\sum_{k=1}^{p-2}\Big(\frac{k(k+1)}{p}\Big) = \sum_{k=1}^{p-2}\Big(\frac{\overline{k}+1}{p}\Big) = \sum_{k=1}^{p-1}\Big(\frac{\overline{k}}{p}\Big) - \Big(\frac{1}{p}\Big) = 0-1 = -1$, car $(\overline{1})^2 = \overline{1}$, donc $\Big(\dfrac{1}{p}\Big) = 1$.

2.a.α) Soit $x \in \mathbb{Z} \setminus p\mathbb{Z}$. Notons $G = \{\overline{x}^k / k \in \mathbb{Z}\}$. G est le groupe multiplicatif engendré par $\overline{x}$ dans $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ (on a bien $\overline{x} \neq 0$). D'après le théorème de Lagrange, $Card(G)$ divise $Card(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}) = p-1$.
De plus d'après le cours sur les groupes cycliques, pour tout $h \in \mathbb{Z}$,
$\overline{x}^h = \overline{1} \Longleftrightarrow Card(G)|h$, donc $\overline{x}^{p-1} = \overline{1}$, ce qu'il fallait démontrer.

2.a.β) Notons g l'application proposée par l'énoncé. Pour tout $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$,
$g(g(x)) = g(x^{-1}\overline{a}) = (x^{-1}\overline{a})^{-1}\overline{a} = x$, donc g est une involution.
Pour tout $x, y \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, notons xRy si et seulement si $[x = y$ ou $y = f(x)]$. En utilisant le fait que $xRy \Longleftrightarrow \{x, f(x)\} = \{y, f(y)\}$, on vérifie que R est une relation d'équivalence, c'est-à-dire que pour tout $x, y, z \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, xRx, $xRy \Rightarrow yRx$ et $[xRy, yRz] \Rightarrow xRz$.
De plus, si $f(x) = x$, alors $x^2 = \overline{a}$, ce qui est faux car $\Big(\dfrac{a}{p}\Big) = -1$, donc les classes d'équivalence sont toutes de cardinal 2.
Comme elles forment une partition de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$,
on a $\overline{(p-1)!} = \displaystyle\prod_{C \in [\mathbb{Z}/p\mathbb{Z}\setminus\{0\}]/R} \prod_{k \in C} k = \prod_{C \in [\mathbb{Z}/p\mathbb{Z}\setminus\{0\}]/R} \overline{a}$, car si C est une classe d'équivalence,

elle est de la forme $C = \{x, f(x)\}$, donc $\prod_{k\in C} k = xf(x) = \overline{a}$.

Finalement, $\overline{(p-1)!} = \overline{a}^{\frac{p-1}{2}}$.

2.a.δ) D'après la question 2.a.α, pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$, x est une racine du polynôme $P = X^{p-1} - 1$, à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}^*$.

Posons $Q = \prod_{x\in\mathbb{Z}/p\mathbb{Z}^*} (X - x)$: P et Q sont tous deux unitaires, donc $\deg(P-Q) < p-1$, or pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$, $(P - Q)(x) = 0$, donc $P - Q$ possède au moins $p - 1$ racines, ce qui d'après le principe de rigidité des polynômes entraîne que $P = Q$. En particulier, $-1 = P(0) = Q(0) = \prod_{x\in\mathbb{Z}/p\mathbb{Z}^*} (-x) = (-1)^{p-1}\overline{(p-1)!}$, or p est impair, donc $(p-1)! \equiv -1\ [p]$.

2.a.γ) Si $\left(\frac{a}{p}\right) = -1$, d'après la question précédente et le théorème de Wilson, modulo p, $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \equiv \left(\frac{a}{p}\right)$.

Si maintenant $\left(\frac{a}{p}\right) = 1$, alors il existe $k \in \mathbb{Z}$ tel que $a \equiv k^2$,

donc $a^{\frac{p-1}{2}} \equiv k^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right)$ d'après le théorème d'Euler.

Remarque : on peut éviter l'utilisation de la question 2.a.β : le point précédent montre que les $\frac{p-1}{2}$ RQ de $\mathbb{Z}/p\mathbb{Z}^*$ sont très exactement les racines du polynôme $X^{\frac{p-1}{2}} - 1$, car il est de degré $\frac{p-1}{2}$, donc il ne peut possèder d'autres racines. Or si x est NRQ dans $\mathbb{Z}/p\mathbb{Z}^*$, alors $(x^{\frac{p-1}{2}})^2 - 1 = 0$, donc $x^{\frac{p-1}{2}} = \pm 1$. Ainsi, $x^{\frac{p-1}{2}} = -1$.

$\diamond$ Modulo 31, $100 \equiv 7$, donc $10^3 \equiv 70 \equiv 8$, donc $\left(\frac{10}{31}\right) \equiv 10^{\frac{31-1}{2}} \equiv (10^3)^5 \equiv 8^5$. De plus, $8^2 = 64 \equiv 2$, donc $8^5 = 8(8^2)^2 \equiv 8 \times 4 \equiv 1$. Ainsi, $\left(\frac{10}{31}\right) \equiv 1$ modulo 31, or $\left(\frac{10}{31}\right) \in \{-1, 1\}$, donc $\left(\frac{10}{31}\right) = 1$.

2.b) p étant impair, $p \equiv 1$ modulo 4 ou $p \equiv 3$.

Supposons d'abord que $p \equiv 1$ modulo 4. Alors $\frac{p-1}{2}$ est pair, donc $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1$ modulo p, or $\left(\frac{-1}{p}\right) \in \{-1, 1\}$, donc $\left(\frac{-1}{p}\right) = 1$.

Supposons maintenant que $p \equiv 3$ modulo 4. Alors $\frac{p-1}{2}$ est impair,

donc $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1$ modulo p, donc $\left(\frac{-1}{p}\right) = -1$.

2.c.α) Supposons qu'aucun diviseur premier de n n'est congru à 3 modulo 4.

$n \equiv 3$ modulo 4, donc n est impair, donc ses diviseurs premiers sont aussi impairs, donc ils sont tous congrus à 1 modulo 4. Ainsi, si p est un diviseur premier de n, dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{p} = \overline{1}$.

D'après le cours, l'entier n se décompose comme un produit de nombres premiers p_i qui sont bien sûr tous des diviseurs premiers de n, donc pour tout i, $\overline{p_i} = \overline{1}$, donc $\overline{3} = \overline{n} = \overline{\prod_i p_i} = \overline{1}$, ce qui est faux. Ainsi, il existe bien un diviseur premier de n qui est congru à 3 modulo 4.

2.c.β) Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de l'équation.
$\diamond$ Supposons que y est pair : il existe $k \in \mathbb{Z}$ tel que $y = 2k$.
Modulo 4, $y^3 = 8k^3 \equiv 0$, donc $x^2 = -1 - y^3 + 8(2z+1)^3 \equiv -1 \equiv 3$. Or, si x est pair $x = 2h$, donc $x^2 = 4h^2 \equiv 0$ modulo 4, et si x est impair, $x = 2h+1$, donc $x^2 = 4h^2 + 4h + 1 \equiv 1$ modulo 4, donc on n'a jamais $x^2 \equiv 3$. Ainsi y est impair.
$\diamond$ On a $x^2 + 1 = (2(2z+1))^3 - y^3 = (2(2z+1) - y)A$,
où $A = (2(2z+1))^2 + y \times 2(2z+1) + y^2 \equiv 2y + y^2$ modulo 4, or y est de la forme $2h+1$, donc $2y = 4h + 2 \equiv 2$ modulo 4 et $y^2 = 4h^2 + 4h + 1 \equiv 1$. Ainsi $A \equiv 3$ modulo 4.
$\diamond$ D'après la question précédente, il existe un nombre premier p, diviseur de A avec $p \equiv 3$ modulo 4. Modulo p, $A \equiv 0$, donc $x^2 + 1 \equiv 0$. Ainsi $-1 \equiv x^2$, donc $\left(\frac{-1}{p}\right) = 1$, ce qui est faux car $p \equiv 3$ modulo 4. On aboutit à une contradiction, sous l'hypothèse que (x, y, z) est une solution de l'équation.
Ainsi cette équation n'a aucune solution dans $\mathbb{Z}^3$.
$\diamond$ Si $(x, y) \in \mathbb{Z}^2$ est une solution de l'équation de Lebesgue, alors $(x, y, 0)$ est une solution de l'équation précédente dans $\mathbb{Z}^3$ ce qui est impossible, donc l'équation de Lebesgue n'admet aucune solution dans $\mathbb{Z}^2$.

3.a)

— 1) $\overline{1} = (\overline{1})^2$, donc $\left(\frac{1}{p}\right) = 1$.

— 2) Si $a \equiv b$ modulo p, alors $\overline{a} = \overline{b}$, donc d'après la fin de l'introduction, a est RQ mod p si et seulement si b est RQ mod p, donc $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

— 3) $\overline{a^2} = (\overline{a})^2$, donc $\left(\frac{a^2}{p}\right) = 1$.

— 4) D'après la question 2), modulo p, $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right)$, or $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$ et $\left(\frac{ab}{p}\right)$ sont dans $\{-1, 1\}$, donc ils sont égaux.

3.b) On a $a = a' \prod_{i=1}^{N} p_i^{s_i}$, avec pour tout $i \in \{1, \ldots, N\}$, s_i pair : posons $s_i = 2t_i$. Ainsi $a = a'b^2$ où $b = \prod_{i=1}^{N} p_i^{t_i}$. Alors d'après la propriété 4) précédente puis la propriété 3), $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a'}{p}\right)$.

4) **Lemme de Gauss**

4.a) Soit $i, j \in \{1, \dots, \frac{p-1}{2}\}$ avec $i > j$. Supposons que $r_i = r_j$. Alors, dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{ia} = \overline{r_i} = \overline{r_j} = \overline{ja}$, donc $\overline{i-j} \times \overline{a} = 0$, or $\overline{a} \neq 0$ et $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $\overline{i-j} = 0$, ce qui est impossible car $1 \leq i - j \leq i \leq \frac{p-1}{2} \leq p - 1$. Ainsi, $r_i \neq r_j$.

4.b)

— 1) Par construction, les entiers $u_1, \dots, u_s, v_1, \dots, v_t$ sont exactement les entiers $r_1, \dots, r_{\frac{p-1}{2}}$ dans un ordre différent, donc ils sont deux à deux distincts et forment $\{r_1, \dots, r_{\frac{p-1}{2}}\}$.

— 2) Soit $i \in \{1, \dots, s\}$ et $j \in \{1, \dots, t\}$. Supposons que $u_i = p - v_j$.
Il existe $k, h \in \{1, \dots, \frac{p-1}{2}\}$ tels que $u_i = r_h$ et $v_j = r_k$.
Alors, dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{h+k} \times \overline{a} = \overline{r_h} + \overline{r_k} = \overline{u_i + v_j} = \overline{p} = 0$, donc $\overline{h+k} = 0$, ce qui est impossible car $1 \leq h + k \leq 2\frac{p-1}{2} = p - 1$. Ainsi $u_i \neq p - v_j$.
De plus, par construction, les $u_1, \dots, u_s$ sont deux à deux distincts, ainsi que les $p - v_1, \dots, p - v_t$, donc les entiers $u_1, \dots, u_s, p - v_1, \dots, p - v_t$ sont deux à deux distincts.
Pour tout $j \in \{1, \dots, t\}$, $\frac{p-1}{2} = p - \frac{p+1}{2} \geq p - v_j \geq p - (p-1) = 1$,
donc $u_1, \dots, u_s, p - v_1, \dots, p - v_t$ constituent $\frac{p-1}{2}$ entiers deux à deux distincts de $\{1, \dots, \frac{p-1}{2}\}$. Ainsi, $\{u_1, \dots, u_s, p - v_1, \dots, p - v_t\} = \{1, \dots, \frac{p-1}{2}\}$.

4.c)

◇ Raisonnons modulo p :
$u_1 \cdots u_s \times v_1 \cdots v_t = r_1 \cdots r_{\frac{p-1}{2}} \equiv a \times (2a) \times \cdots \times (\frac{p-1}{2}a) \equiv a^{\frac{p-1}{2}}(\frac{p-1}{2})!$ et
$(-1)^t u_1 \cdots u_s \times v_1 \cdots v_t \equiv u_1 \cdots u_s \times (p - v_1) \cdots (p - v_t) = 1 \times 2 \times \cdots \times \frac{p-1}{2} \equiv (\frac{p-1}{2})!$,
donc dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^{\frac{p-1}{2}}\overline{(\frac{p-1}{2})!} = (-1)^t\overline{(\frac{p-1}{2})!}$, or dans le corps $\mathbb{Z}/p\mathbb{Z}$,
$\overline{(\frac{p-1}{2})!} = \overline{1} \times \overline{2} \times \cdots \times \overline{\frac{p-1}{2}} \neq 0$, donc $\overline{a}^{\frac{p-1}{2}} = (-1)^t$. Or on a vu que $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$, donc $\left(\frac{a}{p}\right) \equiv (-1)^t$ modulo p, mais $\left(\frac{a}{p}\right)$ et $(-1)^t$ sont dans $\{-1, 1\}$, donc ils sont égaux.

◇ Prenons $p = 29$ et $a = 8$: les restes modulo p de ja pour j variant de 1 à $\frac{p-1}{2} = 14$ sont respectivement, en soulignant ceux qui sont supérieurs à $\frac{p+1}{2} = 15$:
$8, \underline{16}, \underline{24}, 3, 11, \underline{19}, \underline{27}, 6, 14, \underline{22}, 1, 9, \underline{17}, \underline{25}$. Ainsi $t = 7$ puis $\left(\frac{8}{29}\right) = (-1)^7 = -1$.

4.d)

◇ Avec $a = 2$, on a $r_1 = 2$, …, $r_{\frac{p-1}{2}} = 2\frac{p-1}{2} = p - 1$, donc $\left(\frac{2}{p}\right) = (-1)^t$, où t est le nombre des entiers parmi $\{2, 4, \dots, p-1\}$ qui sont supérieurs à $\frac{p}{2}$.
Or pour $n \in \{1, \dots, \frac{p-1}{2}\}$, $2n \leq \frac{p}{2} \iff n \leq \lfloor \frac{p}{4} \rfloor$, donc $t = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$.
◇ Si $p \equiv 1$ modulo 4, alors en posant $p = 1 + 4k$, $p^2 = 1 + 8k + 16k^2$,
donc $\frac{p^2-1}{8} = k + 2k^2 \equiv k$ modulo 2 et $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = 2k - k \equiv -k \equiv k$ modulo 2, donc $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor \equiv \frac{p^2-1}{8}$ modulo 2.
Sinon, $p \equiv 3$ modulo 4, donc en posant $p = -1 + 4k$, $p^2 = 1 - 8k + 16k^2$, donc $\frac{p^2-1}{8} = -k + 2k^2 \equiv k$ modulo 2 et $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = (-1 + 2k) - (k - 1) \equiv k$ modulo 2, donc

on a encore $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor \equiv \frac{p^2-1}{8}$ modulo 2.

◇ Ainsi $\left(\frac{2}{p}\right) = (-1)^t = (-1)^{\frac{p^2-1}{8}}$.

◇ $\left(\frac{8}{31}\right) = \left(\frac{2}{31}\right)^3 = \left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = (-1)^{120} = 1$.

4.e) On suppose que $p = 8n+7$ est premier.

Alors $\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)(p+1)}{8}} = (-1)^{(8n+6)(n+1)} = 1$, mais on a aussi $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$ modulo p, donc $2^{\frac{p-1}{2}} \equiv 1$ modulo p, c'est-à-dire : $p = 8n+7 | 2^{4n+3} - 1$.

Or on peut montrer par récurrence sur n que pour tout $n \in \mathbb{N}^*$, $8n+7 < 2^{4n+3} - 1$, car si $8n+7 < 2^{4n+3} - 1$, alors $2^{4(n+1)+3} - 1 = 2^{4n+3}2^4 - 1 > 2^4(8n+7+1) - 1$, donc $2^{4(n+1)+3} - 1 > 8n + 16 \times 8 - 1 > 8n + 15 = 8(n+1) + 7$.

Ainsi, $2^{4n+3} - 1$ n'est pas un nombre premier.

Partie II

1.a) $\text{Card}\Big(\{a \in \mathbb{N}^* / 0 < a < \frac{p}{2}\}\Big) = \frac{p-1}{2}$ et $\text{Card}\Big(\{b \in \mathbb{N}^* / 0 < b < \frac{q}{2}\}\Big) = \frac{q-1}{2}$, donc $\text{Card}\Big(\{(a,b) \in \mathbb{N}^{*2} / 0 < a < \frac{p}{2} \text{ et } 0 < b < \frac{q}{2}\}\Big) = \frac{p-1}{2} \times \frac{q-1}{2}$.

1.b) Supposons qu'il existe $(m,n) \in \{1, \dots, \frac{p-1}{2}\} \times \{1, \dots, \frac{q-1}{2}\}$ tel que (m,n) soit un point du segment $[O,C]$. Alors $\frac{n}{m} = \frac{q}{p}$, donc $pn = qm$. Ainsi $p | qm$, mais p et q sont premiers entre eux, donc d'après le théorème de Gauss, $p|m$, ce qui est impossible car $1 \leq m \leq p-1$. Ainsi le segment $[O,C]$ ne possède aucun point à coordonnées entières.

1.c) Soit $(j,k) \in \{1, \dots, \frac{p-1}{2}\} \times \{1, \dots, \frac{q-1}{2}\}$. Le point (j,k) est dans le triangle OAC si et seulement si $1 \leq k \leq \frac{q}{p}j$. Pour j fixé, il y a exactement $\lfloor \frac{jq}{p} \rfloor$ entiers k dans $\{1, \dots, \frac{q-1}{2}\}$ vérifiant $k < \frac{jq}{p}$ (on remarque que $\frac{jq}{p} \notin \mathbb{N}$), donc le nombre de points de $\mathbb{N}^{*2}$ situés dans le triangle OAC est $\displaystyle\sum_{j=1}^{\frac{p-1}{2}} \Big\lfloor \frac{jq}{p} \Big\rfloor$.

De même, pour $k \in \{1, \dots, \frac{q-1}{2}\}$ fixé, il y a exactement $\lfloor \frac{kp}{q} \rfloor$ entiers j dans $\{1, \dots, \frac{p-1}{2}\}$ vérifiant $j < \frac{kp}{q}$, donc le nombre de points de $\mathbb{N}^{*2}$ situés dans le triangle OBC est $\displaystyle\sum_{k=1}^{\frac{q-1}{2}} \Big\lfloor \frac{kp}{q} \Big\rfloor$.

4.d)

◇ $(u+v) + (u+pt-v) = 2u + pt \equiv pt$ modulo 2. De plus p est impair, donc $p \equiv 1$ modulo 2, puis $(u+v) + (u+pt-v) \equiv t$ modulo 2.

◇ On a $u + v = \displaystyle\sum_{j=1}^{\frac{p-1}{2}} r_j$ et $u + pt - v = \displaystyle\sum_{i=1}^{s} u_i + \sum_{j=1}^{t} (p - v_j) = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$, donc,

modulo 2, $t \equiv (u+v)+(u+pt-v) \equiv \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j$.

$\diamond$ Pour tout $j \in \{1, \dots, \frac{p-1}{2}\}$, écrivons la division euclidienne de jq par p : $jq = \alpha_j p + r_j$.
Ainsi $\alpha_j = \lfloor \frac{jq}{p} \rfloor$, donc, toujours modulo 2,

$$\sum_{j=1}^{\frac{p-1}{2}} \Big\lfloor \frac{jq}{p} \Big\rfloor \equiv p \sum_{j=1}^{\frac{p-1}{2}} \alpha_j \equiv \sum_{j=1}^{\frac{p-1}{2}} (jq - r_j) \equiv q\frac{p^2-1}{8} - \sum_{j=1}^{\frac{p-1}{2}} r_j \equiv \frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} r_j,$$

ainsi $t \equiv \sum_{j=1}^{\frac{p-1}{2}} \Big\lfloor \frac{jq}{p} \Big\rfloor$.

1.e) On en déduit que $\Big(\frac{q}{p}\Big) = (-1)^t = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor}$.

En échangeant p et q, on a également $\Big(\frac{p}{q}\Big) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor}$,

donc $\Big(\frac{q}{p}\Big)\Big(\frac{p}{q}\Big) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor + \sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor} = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$, d'après la question c.

2.a) $\Big(\frac{q}{p}\Big) = -\Big(\frac{p}{q}\Big)$ si et seulement si $\frac{p-1}{2}\,\frac{q-1}{2}$ est impair, donc si et seulement si $\frac{p-1}{2}$ et $\frac{q-1}{2}$ sont impairs, donc si et seulement si $p \equiv 3$ et $q \equiv 3$ modulo 4.

2.b) $6417 = 3^2.23.31$, donc $\Big(\frac{6417}{6607}\Big) = \Big(\frac{23}{6607}\Big)\Big(\frac{31}{6607}\Big)$.
On a $23 \equiv 3$ modulo 4 et $6607 \equiv 3$ modulo 4, donc $\Big(\frac{23}{6607}\Big) = -\Big(\frac{6607}{23}\Big)$, or $6607 \equiv 6$ modulo 23, donc $\Big(\frac{23}{6607}\Big) = -\Big(\frac{6}{23}\Big) = -\Big(\frac{2}{23}\Big)\Big(\frac{3}{23}\Big)$.
D'après I.4.c, $\Big(\frac{2}{23}\Big) = (-1)^{\frac{23^2-1}{8}} = (-1)^{66} = 1$, de plus $3 \equiv 3$ modulo 4 et $23 \equiv 3$ modulo 4, donc $\Big(\frac{3}{23}\Big) = -\Big(\frac{23}{3}\Big) = -\Big(\frac{2}{3}\Big) = -(-1)^{\frac{3^2-1}{8}} = 1$.
Ainsi, $\Big(\frac{23}{6607}\Big) = -1$.
De plus, $31 \equiv 3$ modulo 4 et $6607 \equiv 3$ modulo 4,
donc $\Big(\frac{31}{6607}\Big) = -\Big(\frac{6607}{31}\Big) = -\Big(\frac{4}{31}\Big) = -\Big(\frac{2^2}{31}\Big) = -1$,
donc finalement, $\Big(\frac{6417}{6607}\Big) = 1$.

3) **Test de Pépin**

◇ Supposons que F_n est premier. Comme $3 \equiv 3$ modulo 4 et $F_n = 2^{2^n} + 1 \equiv 1$ modulo 4 (car $n \geq 1$), on a : $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, or, modulo 3, $F_n \equiv (-1)^{2^n} + 1 \equiv 2$, donc $\left(\frac{3}{F_n}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$, mais on a vu que $\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}}$ modulo F_n, donc $3^{\frac{F_n-1}{2}} \equiv -1$ modulo F_n.

◇ Réciproquement, supposons que $3^{\frac{F_n-1}{2}} \equiv -1$ modulo F_n.

Alors $3^{F_n-1} = \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv 1$ modulo F_n.

Soit p un diviseur premier de F_n (nécessairement $p \geq 5$ car 2 et 3 ne divisent pas F_n). Alors $3^{F_n-1} \equiv 1$ modulo p.

p est premier avec 3, donc $\overline{3} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Si l'on note α l'ordre de $\overline{3}$ pour la multiplication, on sait que $\overline{3}^k = 1 \iff \alpha | k$, donc en particulier, $\alpha | F_n - 1 = 2^{2^n}$.

Mais $3^{\frac{F_n-1}{2}} \equiv -1 \not\equiv 1$ modulo p, donc α ne divise pas $\frac{F_n-1}{2} = 2^{2^n-1}$. Ainsi, $\alpha = 2^{2^n}$.

Mais α est le cardinal du groupe engendré par $\overline{3}$, donc $\alpha \leq p-1$. Ainsi $F_n \leq p$ et $p | F_n$, donc $F_n = p$ est premier.

◇ $F_5 = 2^{2^5} + 1 = 4\ 294\ 967\ 297$.

On calcule $3^{\frac{F_5-1}{2}} = 3^{2^{31}}$ modulo F_5 en utilisant l'algorithme d'exponentiation rapide : on pose $x_0 = 3^{2^0} = 3$ et on définit la suite (x_n) par la relation de récurrence suivante : x_{n+1} est le reste de la division euclidienne de x_n^2 par F_5.

Le programme Python suivant effectue le calcul de x_{31} :

```
x=3
n = 2**(2**5)+1
print('n= ',n)

for i in range(31) :
    x = x**2 % n
    print('3^(2^',i+1,')= ',x)
```

Voici les résultats qu'il produit :

```
n=  4294967297
3^(2^ 1 )=  9
3^(2^ 2 )=  81
3^(2^ 3 )=  6561
3^(2^ 4 )=  43046721
3^(2^ 5 )=  3793201458
3^(2^ 6 )=  1461798105
3^(2^ 7 )=  852385491
3^(2^ 8 )=  547249794
3^(2^ 9 )=  1194573931
3^(2^ 10 )=  2171923848
```

```
3^(2^ 11 )=  3995994998
3^(2^ 12 )=  2840704206
3^(2^ 13 )=  1980848889
3^(2^ 14 )=  2331116839
3^(2^ 15 )=  2121054614
3^(2^ 16 )=  2259349256
3^(2^ 17 )=  1861782498
3^(2^ 18 )=  1513400831
3^(2^ 19 )=  2897320357
3^(2^ 20 )=  367100590
3^(2^ 21 )=  2192730157
3^(2^ 22 )=  2050943431
3^(2^ 23 )=  2206192234
3^(2^ 24 )=  2861695674
3^(2^ 25 )=  2995335231
3^(2^ 26 )=  3422723814
3^(2^ 27 )=  3416557920
3^(2^ 28 )=  3938027619
3^(2^ 29 )=  2357699199
3^(2^ 30 )=  1676826986
3^(2^ 31 )=  10324303
```

Ainsi, $3^{\frac{F_5-1}{2}} = 3^{2^{31}} \equiv 10\ 324\ 303 \not\equiv -1$ modulo 4 294 967 297, donc F_5 est composé.

4.a) Il nous faut discuter suivant la congruence de p modulo 4, pour utiliser la loi de réciprocité quadratique, et la congruence de p modulo 3, pour simplifier $\left(\frac{p}{3}\right)$, d'où une discussion selon la valeur de p modulo 12.
Si $p \equiv -1$ modulo 12, il existe $k \in \mathbb{N}^*$ tel que $p = 12k - 1$.
Modulo 4, on a $3 \equiv 3$ et $p \equiv 3$, donc $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, mais $p \equiv -1$ modulo 3, donc $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = -1$ (déjà vu). On en déduit que $\left(\frac{3}{p}\right) = 1$.
Les autres cas se traitent de façon analogue.
4.b) $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ ce qui permet de conclure en utilisant les questions I.2.b et II.4.a.