DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Noé DE RANCOURT
STAGE : Montpellier 2012

Cyclicité de $\mathbb{Z}/p\mathbb{Z}$

- Racine primitive -

Soit $n > 1$ et a premier avec n. Dans le premier cours vous avez vu $\omega_n(a)$ l'ordre de a modulo n et vous savez que cet ordre est un diviseur de $\varphi(n)$. Ici nous chercherons des éléments dont l'ordre est pile $\varphi(n)$. Dans la suite de ce cours nous noterons $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles (c-à-d premiers avec n).

Définition 1. Soit n un entier et x premier avec n. On dit que x est une *racine primitive* modulo n si l'ordre de x est $\varphi(n)$.

Définition 2. Soit n un entier. On dit que $\mathbb{Z}/n\mathbb{Z}$ est *cyclique* s'il existe une racine primitive modulo n.

Essayons d'expliquer pourquoi nous utilisons le nom "cyclique". Soit x une racine primitive, considérons $x, x^2, x^3, \ldots, x^{\varphi(n)}$. Tous ces points sont des éléments de $\mathbb{Z}/n\mathbb{Z}$ distincts deux à deux et premiers avec n, donc il s'agit de tous les éléments premiers avec n. De plus si on note $a = x^\alpha$, $b = x^\beta$, $c = x^\gamma$, on aura alors :

$$a \times b \equiv c[n] \iff \alpha + \beta \equiv \gamma[\varphi(n)].$$

Tous les éléments inversibles peuvent donc être placés sur un cycle de taille $\varphi(n)$, l'étude de $(\mathbb{Z}/n\mathbb{Z})^*$ revient juste à l'étude de $\mathbb{Z}/\varphi(n)\mathbb{Z}$, que vous connaissez bien.

Commençons par montrer une proposition sur les ordres.

Proposition 3. Soit $n > 1$, et a, b premiers avec n d'ordres respectifs u et v. Alors il existe un élément c d'ordre $\mathrm{ppcm}(u, v)$.

Démonstration. Intéressons nous d'abord au cas où u et v sont premiers entre eux et regardons w l'ordre de ab. Il est facile de vérifier que $(ab)^{uv} \equiv 1[n]$, donc $w|uv$. Montrons à présent que $u|w$:

$$(ab)^w \equiv 1[n] \implies a^w \equiv b^{-w}[n] \implies a^{wv} \equiv b^{-wv} \equiv 1[n] \implies u|wv \implies u|w$$

L'avant-dernière implication vient de la proposition $a^k \equiv 1[n] \iff \omega_n(a)|k$, et la dernière par l'hypothèse que u et v premiers entre eux. Donc $u|w$ et $v|w$, mais $w|uv$, donc $w = uv$, ce qui achève la démonstration.

Regardons maintenant le cas où u et v ne sont pas premiers entre eux, soit $d = pgcd(u, v)$. Je vous laisse vérifier que a^d a pour ordre $\frac{u}{d}$, et que $\frac{u}{d}$ et v sont premiers entre eux. Par le paragraphe précédent, il existe un élément d'ordre $\frac{uv}{d} = ppcm(u, v)$.

Revenons maintenant au problème qui nous intéresse. Pour $n > 1$, nous définissons l'ordre maximal modulo n

$$\Omega_n = \max_{a \text{ premier avec } n} \omega_n(a).$$

Proposition 4.

$$\Omega_n = ppcm\{\omega_n(a) | a \text{ premier avec } n\}$$

Cette proposition découle facilement de la précédente.

On voit que si Ω_n est l'ordre maximal mod n, alors l'ordre de tous les éléments est un diviseur de Ω_n, ou encore que tous les éléments inversibles a vérifient

$$a^{\Omega_n} \equiv 1[n].$$

- Cyclicité de $\mathbb{Z}/p\mathbb{Z}$ -

Je vous renvoie au cours précédent pour montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps (c'est-à-dire que tous les éléments sont inversibles) et que par conséquent on peut utiliser les polynômes comme si on était sur les réels. La propriété qui nous intéressera est qu'un polynôme de degré n a au plus n racines.

Remarque 5. Les polynômes ici ne sont pas sur des entiers mais sur des classes de congruences mod p. Ainsi k et $k+p$ ne comptent que pour une seule racine.

Théorème 6. Soit p un premier, $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Démonstration. Soit Ω_p l'ordre maximal modulo p. Tout d'abord, $\Omega_p|(p-1)$. Ensuite, d'après la section précédente, tous les entiers a premiers avec p

vérifient $a^{\Omega_p} \equiv 1[p]$. Le polynôme $X^{\Omega_p} - 1$ a donc $(p-1)$ racines. Ainsi $\Omega_p \geqslant (p-1)$, le seul cas possible est $\Omega_p = p-1$. Il existe donc un élément de $\mathbb{Z}/p\mathbb{Z}$ d'ordre $p-1$, $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Illustrons ce résultat par un exemple, avec $p = 7$. Un peu de tâtonnement permet de trouver que 3 est racine primitive modulo p et on trouve

$$3^0 \equiv 1\ ;\ 3^1 \equiv 3\ ;\ 3^2 \equiv 2\ ;\ 3^3 \equiv 6\ ;\ 3^4 \equiv 4\ ;\ 3^5 \equiv 5$$

Donc pour chaque élément a de $\mathbb{Z}/7\mathbb{Z}$ on associe α l'exposant tel que $a = 3^\alpha$. Ainsi nous pouvons traduire des égalités de produits par des égalités sur les exposants. Par exemple, avec a, b, c premiers avec p

$$4a^2b \equiv 6c^3[7] \iff 4 + 2\alpha + \beta \equiv 3 + 3\gamma[6].$$

Nous pouvons écrire le résultat de cette façon :

$$((\mathbb{Z}/p\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +).$$

Cette écriture signifie qu'il existe une bijection f de $(\mathbb{Z}/p\mathbb{Z})^*$ vers $\mathbb{Z}/((p-1))\mathbb{Z}$ qui transforme l'opération $\times$ en $+$, c-à-d pour tout a, b $f(a \times b) = f(a) + f(b)$ et $f(1) = 0$ (f conserve les neutres, 1 est le neutre pour $\times$ et 0 est le neutre pour $+$).

La ligne se lit de cette façon : "le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ muni de la multiplication est isomorphe au groupe $\mathbb{Z}/(p-1)\mathbb{Z}$ muni de l'addition".

- Cyclicité de $\mathbb{Z}/p^k\mathbb{Z}$ (p premier impair) -

Dans tout ce chapitre, p sera un nombre premier *impair*. Rappellons rapidement que $\varphi(p^k) = (p-1)p^{k-1}$.

Proposition 7. L'ordre de $(p+1)$ modulo p^k est p^{k-1}.

Démonstration. Regardons ce que vaut $(1+p)^{p^{k-1}}$:

$$\begin{aligned}(1+p)^{p^{k-1}} &= 1 + \binom{p^{k-1}}{1}p + \binom{p^{k-1}}{2}p^2 + \binom{p^{k-1}}{3}p^3 + \dots \\ &= 1 + p^k + p^{k+1} \cdot \frac{p-1}{2} + p^{k+2} \cdot \frac{(p-1)(p-2)}{6} + \dots\end{aligned}$$

Nous voyons que la puissance de p augmente de plus en plus lorsqu'on va vers la droite. Je vous laisse vous convaincre du résultat suivant :

$$(1+p)^{p^{k-1}} = 1 + \lambda \cdot p^k \text{ avec } p \not| \lambda.$$

Ce résultat nous dit déjà que l'ordre de $(1+p)$ modulo p^k est un diviseur de p^{k-1}, c'est à dire une puissance de p. Si on suppose que l'ordre de $(1+p)$ est strictement plus petit que p^{k-1}, alors l'ordre serait un diviseur de p^{k-2} et on aurait

$$(1+p)^{p^{k-1}} = \left((1+p)^{p^{k-2}}\right)^p = (1+\mu\cdot p^k)^p = \cdots = 1+\nu\cdot p^{k+1},$$

ce qui est en contradiction avec le résultat précédent. Donc l'ordre de $(p+1)$ modulo p^k est p^{k-1}.

Maintenant, pour obtenir $\varphi(p^k)$, il ne nous manque qu'un facteur $(p-1)$. Dans la section précédente nous avons montré qu'il est toujours possible de trouver une racine d'ordre $(p-1)$ modulo p. Donc prenons un entier a qui est une racine primitive modulo p et regardons ω son ordre modulo p^k :

$$a^\omega \equiv 1[p^k] \implies a^\omega \equiv 1[p] \implies (p-1)|\omega.$$

Théorème 8. Soit p un premier impair et $k \geqslant 1$ un entier, $\mathbb{Z}/p^k\mathbb{Z}$ est cyclique.

Démonstration. Regardons ce que nous avons : nous savons que tous les ordres modulo p^k divisent $\varphi(p^k) = (p-1)p^{k-1}$, et nous avons un élément d'ordre p^{k-1} et un élément dont l'ordre est un multiple de $p-1$. Par la première propriété du cours il existe un élément dont l'ordre est le ppcm des deux, qui sera exactement $(p-1)p^{k-1}$.

Comme pour la section précédente, écrivons ce résultat sous forme d'un isomorphisme de groupes :

$$((\mathbb{Z}/p^k\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/((p-1)p^{k-1})\mathbb{Z}, +).$$

- Structure de $(\mathbb{Z}/2^k\mathbb{Z})^*$ -

Commençons par regarder l'exemple de $\mathbb{Z}/8\mathbb{Z}$. Cherchons une racine primitive, c-à-d un élément d'ordre 4.

$$1^1 \equiv 1[8]\ ;\ 3^2 = 9 \equiv 1[8]\ ;\ 5^2 = 25 \equiv 1[8]\ ;\ 7^2 = 49 \equiv 1[8],$$

tous les éléments sont d'ordre 1 ou 2. Donc $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique. La structure de $(\mathbb{Z}/2^k\mathbb{Z})^*$ est un peu plus compliquée.

Théorème 9. Soit $k \geqslant 3$,

$$((\mathbb{Z}/2^k\mathbb{Z})^*, \times) \simeq ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}), +).$$

Expliquons ce qu'est $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$. Il s'agit de tous les couples $(\varepsilon; \alpha)$ avec $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$ et $\alpha \in \mathbb{Z}/2^{k-2}\mathbb{Z}$. L'addition se fait de la manière suivante :

$$(\varepsilon; \alpha) + (\varepsilon'; \alpha') = \left(\varepsilon + \varepsilon'[2]; \alpha + \alpha'[2^{k-2}]\right).$$

Démonstration abrégée. Nous n'allons pas faire cette démonstration dans son intégralité, mais voici les points importants :

- Utiliser l'exemple de $\mathbb{Z}/8\mathbb{Z}$ pour prouver qu'il est impossible que $(\mathbb{Z}/2^k\mathbb{Z})$ soit cyclique
- Montrer que $5 = (1 + 4)$ est d'ordre 2^{k-2} de la même façon qu'on avait montré l'ordre de $(1 + p) \bmod p^k$
- Montrer que la fonction

$$\begin{array}{rccc} f: & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}) & \to & (\mathbb{Z}/2^k\mathbb{Z})^* \\ & (\varepsilon, \alpha) & \mapsto & \epsilon \cdot 2^{k-1} + 5^\alpha \end{array}$$

  est un isomorphisme de groupe (c-à-d que f est une bijection qui transform $+$ en $\times$).

- Exercices -

Certains des exercices sont sur les résultats du cours précédent. Au début de chaque sous-section j'ai mis le résultat dont vous avez besoin.

Cyclicité de $\mathbb{Z}/p\mathbb{Z}$

Théorème 10. Soit p un nombre premier impair et $k \geqslant 1$. Le groupe $\mathbb{Z}/p^k\mathbb{Z}$ est cyclique, c'est-à-dire qu'il existe une racine primitive x telle que la famille $(x^n)_{n\in\mathbb{N}}$ va passer par toutes les classes d'equivalence (premières avec p) modulo p^k. On peut considérer que

$$((\mathbb{Z}/p^k\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/((p-1)p^{k-1})\mathbb{Z}, +).$$

Pour les puissances de 2 c'est un peu plus compliqué : si $k \geqslant 3$,

$$((\mathbb{Z}/2^k\mathbb{Z})^*, \times) \simeq \left((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}), +\right).$$

Exercice 1 Combien y a-t-il de classes a modulo 343 telles que $a^{70} \equiv 1[343]$? Même question modulo 128.

Exercice 2 Soit n divisible par deux premiers impairs distincts. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

Exercice 3 Déterminer tous les entiers n tels qu'il existe un entier a vérifiant $a^{\frac{\varphi(n)}{2}} \equiv -1[n]$ (φ est l'indicatrice d'Euler).

Exercice 4 Trouver les entiers n tels que $37|2 \cdot 6^{4n+3} + 2^n$.

Exercice 5 Trouver tous les couples (a, b) solutions de $a^3 \equiv b^3[121]$. Même questions avec [169].

Résidus quadratiques

Théorème 11. (Réciprocité quadratique) Soient p et q deux nombres premiers impairs distincts. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre. Vous pouvez utiliser les trois formules suivantes :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \; ; \; \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1)}{2}} \; ; \; \left(\frac{2}{p}\right) = (-1)^{fracp^2-1)8}$$

Exercice 6 Quand 5 est-il un carré mod p ? Et 7 ? Et les deux ?

Exercice 7 Calculer $\left(\frac{37}{97}\right)$.

Exercice 8 Combien y a-t-il de "résidus quadratiques" mod pq ? Et mod p^n ?

Exercice 9 Trouver les solutions entières de $4x^2 + 77y^2 = 487z^2$.

Lemme LTE

Lemme 12. (Lifting The Exponent) Soit p un nombre premier impair et x, y deux entiers tels que $p|x - y$ mais $p \not| x$, $p \not| y$. Alors

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n)$$

Exercice 10 Trouver les entiers n tels qu'il existe x, y, k avec $x$et y premiers entre eux et

$$3^n = x^k + y^k.$$

Exercice 11 Soit p un premier impair et m un entier tel qu'il existe des entiers $x, y > 1$ vérifiant

$$\frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m.$$

Montrer que $m = p$.

Exercice 12 Trouver toutes les solutions entières de

$$x^{2009} + y^{2009} = 7^k$$

- Corrigé des exercices -

Solution de l'exercice 1 Tout d'abord, $343 = 7^3$, le groupe $(\mathbb{Z}/343\mathbb{Z})^a st$ est donc cyclique et isomorphe à $\mathbb{Z}/294\mathbb{Z}$ ($294 = 6 \cdot 7^2$). Soit x une racine primitive et α tel que $a = x^\alpha$:

$$a^{70} \equiv 1[343] \iff 70\alpha \equiv 0[294] \iff 21|\alpha,$$

ce qui nous donne 14 classes d'équivalences mod 294 pour α qui correspondent à 14 classes d'équivalence modulo 343 pour a.

Maintenant, pour le modulo 128, c'est légèrement différent puisque

$$((\mathbb{Z}/128\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(32)\mathbb{Z}, +).$$

On cherche donc tous les couples (ε, k) avec $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$ et $k \in \mathbb{Z}/32\mathbb{Z}$ qui vérifient $70\varepsilon \equiv 0[2]$ et $70k \equiv 0[32]$. On voit rapidement que l'on a deux choix pour ε et deux choix pour k, ce qui correspond à 4 classes d'équivalence mod 128.

Solution de l'exercice 2 Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition en facteurs premiers de n. Je vous laisse utiliser le théorème chinois pour montrer que pour tout a, si on note $\omega_j(a)$ l'ordre de a mod j :

$$\omega_n(a) = ppcm\left(\omega_{p_1^{\alpha_1}}(a), p_2^{\alpha_2}(a), \dots, p_k^{\alpha_k}(a)\right).$$

Comme l'ordre d'un élément mod j divise $\varphi(j)$, on a que

$$\omega_n(a) \left| ppcm\left((p_1 - 1)p_1^{\alpha_1 - 1}, (p_2 - 1)p_2^{\alpha_2 - 1}, \dots, (p_k - 1)p_k^{\alpha_k - 1}\right)\right.$$

Or on veut un élément dont l'ordre soir $\varphi(n)$, qui est le produit des termes de droite. Le $ppcm$ de ces termes est égal à leur produit ssi ils sont tous premiers entre eux deux à deux, mais il est facile de voir que si n est divisible par deux premiers impairs distincts, deux de ces termes sont pairs. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

Je vous laisse faire la généralisation suivante : $\mathbb{Z}/n\mathbb{Z}$ est cyclique ssi $n = 2, 4, p^k$ ou $2p^k$.

Solution de l'exercice 3 On veut un entier a tel que $a^{\frac{\varphi(n)}{2}} \equiv -1[n]$, donc que $\omega_n(a) \not| \frac{\varphi(n)}{2}$. On utilise la même technique que précédemment pour calculer l'ordre maximal mod n en fonction de la décomposition en facteurs premiers de n, et on voit que les seuls n possibles sont 4, p^k et $2p^k$ (p premier impair).

Solution de l'exercice 4 Ici il n'y a rien de sorcier, nous allons regarder les suites des 6^m et 2^n modulo 37 :

$$6 \to 36 = -1 \to -6 \to 1 \to 6 \to -1 \to \dots$$

donc $2 \cdot 6^{4n+3}$ est toujours congru à 12 mod 37.

$$2 \to 4 \to 8 \to 16 \to 32 \to 27 \to 17 \to 34 \to 31 \to 25 \to 13 \to 26 \to 15 \to 30 \to 23 \to 9 \to 1$$

avec après la même suite mais avec des moins partout. Donc l'ordre de 2 est 36, et $2^n \equiv -12[37]$ ssi $n \equiv 10[36]$.

Solution de l'exercice 5 Tout d'abord, on écarte les cas divisibles par 11 : si a et b sont divisibles par 11, l'équation est vérifiée. Maintenant on s'intéresse à ceux qui sont premiers avec 11. Comme 121 est une puissance de 11, on peut utiliser la cyclicité de $(\mathbb{Z}/p^k\mathbb{Z})^*$. Soit x une racine primitive et α, β tels que $a = x^\alpha$, $b = x^\beta$.

$$a^3 \equiv b^3[121] \iff 3\alpha \equiv 3\beta[110] \iff \alpha \equiv \beta[110]$$

la dernière équivalence puisque 3 est premier avec 110. Donc $a^3 \equiv b^3[121]$ ssi $a \equiv b[121]$ou a, b multiples de 11.

Pour 169, le cas a et b sont divisibles par 13 reste le même. Maintenant regardons la cyclicité avec les mêmes notations.

$$a^3 \equiv b^3[169] \iff 3\alpha \equiv 3\beta[156] \iff \alpha \equiv \beta[52]$$

il y a donc plus de solutions : $\alpha \equiv \beta[156]$, $\alpha \equiv \beta + 52[156]$ ou $\alpha \equiv \beta + 104[156]$. Pour voir à quoi cela correspond mod 169, il faut trouver une racine troisième de l'unité mod 169, 22 marche ($22^2 \equiv 146$, $22^3 \equiv 1$). Les solutions sont donc : a, b multiples de 13 ou $a \equiv b[169]$ ou $a \equiv 22 \cdot b[169]$ ou $a \equiv 146 \cdot b[169]$.

Solution de l'exercice 6 Nous allons utiliser la réciprocité quadratique : $\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = 1$ puisque $5 \equiv 1[4]$, donc 5 est un carré mod p ssi p est un carré mod 5 ssi $p \equiv \pm 1[5]$.

Même topo pour 7 mais il faut faire une disjonction de cas :

- si $p \equiv 1[4]$, alors $\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = 1$ et 7 est un carré mod p ssi p est un carré mod 7 ssi $p \equiv 1, 2$ ou $4[7]$.
- si $p \equiv 3[4]$, alors $\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = -1$ et 7 est un carré mod p ssi p n'est pas un carré mod 7 ssi $p \equiv 3, 5$ ou $6[7]$.

Nous pouvons tout regrouper en disant que 7 est un carré mod p ssi $p \equiv 1, 3, 9, 19, 25$ ou $27[28]$.

Pour que 5 et 7 soient tous les deux des carré mod p, il faut que les deux conditions soient vérifiées. Je laisse au lecteur le soin de déterminer les 12 classes d'équivalences mod 140 que cela donnera en utilisant le théorème chinois.

Solution de l'exercice 7 Appliquons la réciprocité quadratique :

$$\begin{array}{rcll}
\left(\frac{37}{97}\right) & = & \left(\frac{97}{37}\right) & \text{puisque } \left(\frac{37}{97}\right)\left(\frac{97}{37}\right) = 1 \\
& = & \left(\frac{23}{37}\right) & \text{puisque seule la classe de 97 mod 37 compte} \\
& = & \left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) & \text{puisque } \left(\frac{37}{23}\right)\left(\frac{23}{37}\right) = 1 \\
& = & \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) & \text{puisque le symbole de Legendre est multiplicatif} \\
& = & \left(\frac{2}{23}\right) \cdot -\left(\frac{23}{7}\right) & \text{puisque } \left(\frac{7}{23}\right)\left(\frac{23}{7}\right) = -1 \\
& = & -1 & \text{puisque } \left(\frac{2}{23}\right) = 1 \text{ et } \left(\frac{2}{7}\right) = 1
\end{array}$$

Solution de l'exercice 8 Nous allons juste considérer que les "résidus quadratiques" mod n sont parmi les entier premiers avec n. La technique pour étudier $\mathbb{Z}/pq\mathbb{Z}$ est d'étudier séparément $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ et d'utiliser le théorème chinois. Je laisse au lecteur le soin de vérifier que a résidu quadratique mod pq ssi a résidu quadratique mod p et a résidu quadratique mod q. Modulo p il y a $\frac{p-1}{2}$ résidus quadratiques, et mod q il y en a $\frac{q-1}{2}$. Le nombre total de résidus quadratiques mod pq est donc $\frac{(p-1)(q-1)}{4}$.

Pour regarder mod p^k nous allons procéder autrement et profiter du fait que $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique. On écrit tous les élements comme les puissances x^n d'une racine primitive x. Il est facile de vérifier que x^n est un résidu quadratique ssi n est pair. Les résidus quadratiques correspondent donc à la moitié des éléments, c'est-à-dire $\frac{(p-1)p^{k-1}}{2}$.

Solution de l'exercice 9 Nous allons profiter que 487 est un carré. L'ésuation implique que $4x^2 = -77y^2[487]$, donc si -77 n'est pas un carré mod 487, l'équation n'a pas de solutions. Je laisse au lecteur le soin de vérifier que $\left(\frac{-77}{487}\right) = -1$.

Solution de l'exercice 10 Tout d'abord, k doit être impair. En effet si k était pair, x^k et y^k seraient des carrés et il est facile de vérifier $3|a^2 + b^2 \implies 3|a$ et $3|b$ (il suffit de vérifier toutes les congruences possibles mod 3 pour a et b). Supposons qu'il existe un premier impair p qui divise $x + y$, alors par le lemme LTE, on aurait

$$v_p(3^n) = v_p(x^k + y^k) = v_p(x + y) + v_p(k) \geqslant 1.$$

On en déduit donc que $p|3^n$, et donc $p = 3$. Cela signifie que $x + y = 3^m$, pour un entier positif m. On remarque que $n = v_3(k) + m$. Distinguons deux cas :

– si $m > 1$: Je vous laisse prouver que $3^a \geqslant a+2$ et donc $v_3(k) \leqslant k-2$. On peut supposer $x > y$ et comme $x+y = 3^m \geqslant 9$, on aura $x \geqslant 5$, mais aussi $x > \frac{3^m}{2}$. Nous utilisons maintenant quelques inégalités :

$$x^k + y^k \geqslant x^k \geqslant \frac{3^m}{2} 5^{k-1} > 3^m 5^{k-2} \geqslant 3^{m+v_3(k)} = 3^n$$

ce qui est une contradiction.
– si $m = 1$, alors on a $x = 2$ et $y = 1$, et $3^{1+v_3(k)} = 1 + 2^k$. On remarque que $3^{1+v_3(k)} | k$, donc $3^{1+v_3(k)} \leqslant k$ et $2^k + 1 \leqslant 3k$, et donc $k \leqslant 3$. Il ne reste pas beaucoup de cas à vérifier et la seule solution est :

$$3^2 = 1^3 + 2^3.$$

<u>*Solution de l'exercice 11*</u> Par la convexité de $x \mapsto x^p$, $\frac{x^p+y^p}{2} \geqslant \left(\frac{x+y}{2}\right)^p$. Donc comme $\frac{x^p+y^p}{2} = \left(\frac{x+y}{2}\right)^m$ il s'ensuit que $m \geqslant p$. Soit $d = pgcd(x,y)$, $x = dx'$, $y = dy'$. L'équation se réécrit

$$2^{m-1}(x'^p + y'^p) = d^{m-p}(x'+y')^m.$$

Soit q un diviseur premier impair de $x'+y'$. Par le lemme LTE, $v_q(x'^p + y^p) = v_q(x+y) + v_q(p)$ et d'autre part $v_q(d^{m-p}(x'+y')^m) \geqslant m v_q(x+y)$. Donc $m \geqslant 2$ et $p \geqslant 2$, ce qui aboutit à une contradiction. À présent regardons v_2 : on obtient

$$m - 1 + v_2(x'+y') \geqslant m v_2(x'+y'),$$

donc $v_2(x'+y') \leqslant 1$, $x'+y' \leqslant 2$, donc $x' = y' = 1$ et $m = p$.

<u>*Solution de l'exercice 12*</u> Déjà, $2009 = 7^2 \times 41$. Comme $x+y$ divise $x^{2009} + y^{2009}$, $x+y$ est une puissance de 7. On remarque aussi que si x et y sont multiples de 7, on peut tout diviser par 7 et juste changer l'exposant k ; on peut donc supposer que x et y sont premiers avec 7. Le lemme LTE nous dit que $v_7(x^{2009} + y^{2009}) = v_7(x+y) + v_7(2009) = v_7(x+y) + 2$, donc $x^{2009} + y^{2009} = 49(x+y)$, donc

$$\frac{x^{2009} + y^{2009}}{x+y} = x^{2008} - x^{2007}y + x^{2006}y^2 - \cdots + y^{2008} = 49$$

Mais il estfacile de vérifier que ce terme est beaucoup plus grand que 49. Par exemple, si on suppose $x > y$, on aura toujours $(x^{2008} - x^{2007}y) \geqslant 1$; $(x^{2006}y^2 - x^{2005}y^3) \geqslant 1$ et ainsi de suite, la somme totale sera au moins égale à 1004. Il n'y a donc pas de solutions possibles.