# Arithmétique & groupes

Marc SAGE

$1^{\text{ier}}$ juillet 2008

## Table des matières

Les pgcd et ppcm de deux entiers $a$ et $b$ seront notés

$$\begin{cases} a \wedge b := \text{pgcd}\,(a,b) \\ a \vee b := \text{ppcm}\,(a,b) \end{cases}.$$

Pour un entier $n \geq 2$ et $p$ un nombre premier, on rappelle que la *valuation* $p$-adique, notée $v_p(n)$, est la puissance de $p$ qui apparaît dans la décomposition de $n$ en facteurs premiers, de sorte que tout entier s'écrit

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

Pour $p$ premier, le corps[1] à $p$ éléments sera noté

$$\mathbb{F}_p := {}^{\mathbb{Z}}\!\diagup_{p\mathbb{Z}}.$$

# 1 Mise en jambe

1. *Quels sont les entiers $n \geq 2$ tels que $\frac{3^n - 2^n}{n}$ soit entier ?*
2. *Soit $p \geq 3$ un premier. Montrer que le numérateur de la fraction suivante est un multiple de $p$ :*

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots + \frac{1}{(p-1)^3}.$$

3. *montrer que pour $p \geq 5$ premier, $\binom{2p}{p} = 2$ modulo $p^3$.*

**Solution proposée.**

1. Soit $n$ un tel entier et $p$ un premier divisant $n$. On a donc $3^n = 2^n$ modulo $p$. En particulier, $p$ n'est pas 2 (sinon $1^n = 0^n$ modulo 2), donc 2 est inversible dans $\mathbb{F}_p^*$, d'où $\left(\frac{3}{2}\right)^n = 1$. L'ordre de $\frac{3}{2}$ doit donc diviser $n$, mais comme il divise toujours[2] $p-1$, on a trouvé un diviseur de $n$ qui est $< p$. En choisissant rétrospectivement $p$ minimal, ce diviseur doit valoir 1, d'où $\frac{3}{2} = 1$ et $3 = 2$ modulo $p$, ce qui est impossible.
2. rq : $\frac{a}{b} = \frac{c}{d}$Observer que le dénominateur commun $d^3 := (p-1)!^3$ n'est pas nul modulo $p$, de sorte que la conclusion est invariante par multiplication par un non-multiple de $p$. Pour tuer les fractions, on regarde $d^3 \sum_{1 \leq k < p} \frac{1}{k^3}$. Mq $\sum \left(\frac{d}{k}\right)^3 = 0$ dans $\mathbb{F}_p^*$. $k \mapsto \frac{d}{k}$ est une involution de $\mathbb{F}_p^*$, donc une bijection, d'où $\sum \left(\frac{d}{k}\right)^3 = \sum k^3 = \left(\frac{p(p-1)}{2}\right)^2 = 0$ car $p$ impair, *CQFD*.
3. Mêmem idée : on tuer le dénom $d := (p-1)!$ pour se ramener dans $\mathbb{F}_p^*$ : on a les égalités

$$d\binom{2p}{p} = d\sum_0^p \binom{p}{k}^2 = 1 + p^2 \sum_1^{p-1} \left((p-1)^{\downarrow k-1} \frac{d}{k!}\right)^2 + 1$$

La somme à l'intérieur vaut (modulo $p$)

$$\sum_{0<k<p} \left((p-1)^{\downarrow (k-1)} \frac{d}{k!}\right)^2 = \sum_{0<k<p} \left((-1)^{\downarrow k-1} \frac{d}{k!}\right)^2 = \sum_{0<k<p} \left((-1)^{k-1} (k-1)! \frac{d}{k!}\right)^2 = \sum_{0<k<p} \left(\frac{d}{k}\right)^2 = \sum_{0<k<p} k^2 = p\frac{p-1}{2}$$

Or, 2 divse $p-1$, et 3 divise l'un des deux numérateurs (distniguer les cas)

Rq : bonne faon de faire est de considérer les fractions de $Q$ de dénom $\notin pZ$ : c'est un anneau, et on vérifie aisément que la projection mod $p$ est un morphisme d'anneau. Plus généraliemnt, tout morphisme d'anneau intéègre induit morphisme du localisé en le noyau (qui est idéal premier) dans le corps des fraciton à l'arrivée.

[1] Le terme mathématique « corps » se dit "**f**ield" en anglais, d'où la lettre $\mathbb{F}$ choisie pour $\mathbb{F}_p$.
[2] C'est le petit théorème de Fermat, cas particulier du théorème de Lagrange appliqué au groupe $\mathbb{F}_p^*$.

## 2 Sur l'indicatrice d'Euler

Pour $n$ un entier $\geq 1$, on note $\varphi(n)$ le nombre d'entiers parmi $\{1, ..., n\}$ qui sont premiers avec $n$. $\varphi$ est appelée *indicatrice d'Euler*. On rappelle que $\varphi(n)$ désigne également le cardinal $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

*Montrer que $\varphi$ est multplicative.*

résulte immédiatement du théorème chinois.

## 3 Calcul des sommes de Newton dans $\mathbb{F}_p$

*Calculer $S_k := \sum_{x\in\mathbb{F}_p} x^k$ pour $k \in \mathbb{Z}$, selon que $p-1$ divise $k$ ou non.*

**Solution proposée.**

*Première méthode (groupes).*

Laissons déjà de côté le cas $k = 0$ qui donne

$$S_0 = \sum_{x\in\mathbb{F}_p} x^0 = \sum_{x\in\mathbb{F}_p} 1 = |\mathbb{F}_p| = p = 0.$$

On peut alors indexer la somme sur le groupe $\mathbb{F}_p^*$ vu que $0^k = 0$. Un argument classique consiste alors à dire que, puisqu'un groupe est invariant par translation d'un élément quelconque $a$, on a

$$S_k = \sum_{x\in\mathbb{F}_p^*} x^k = \sum_{x\in\mathbb{F}_p^*} (ax)^k = \sum_{x\in\mathbb{F}_p^*} a^k x^k = a^k S_k.$$

Ainsi, ou bien il y a un $a \in \mathbb{F}_p^*$ tel que $a^k \neq 1$ et alors $S_k = 0$, ou bien $a^k = 1$ pour tout $a \in \mathbb{F}_p^*$ et alors $S_k = 1 + ... + 1 = p - 1 = -1$. On a donc

$$S_k = \begin{cases} 0 \text{ si } \exists a \in \mathbb{F}_p^*,\ a^k \neq 1 \\ -1 \text{ si } \forall a \in \mathbb{F}_p^*,\ a^k = 1 \end{cases}.$$

Précisons ces deux conditions selon que $p-1$ divise $k$ ou pas.

Supposons $p-1 \mid k$. Alors pour tout $a$ dans $\mathbb{F}_p^*$, le PTF[3] nous donne

$$a^k = \left(a^{p-1}\right)^{\frac{k}{p-1}} = 1^{\frac{k}{p-1}} = 1.$$

Suppposons réciproquement que $\forall a \in \mathbb{F}_p^*,\ a^k = 1$. L'ordre de tout $a \in \mathbb{F}_p^*$ doit donc diviser $k$, et comme il divise également $p-1$ par le PTF, les ordres des $a \in \mathbb{F}_p^*$ doivent diviser le pgcd $d := k \wedge (p-1)$. Ainsi, le polynôme $X^d - 1$ s'annule sur $\mathbb{F}_p^*$, donc a au moins $p-1$ racines, d'où $p-1 \leq d$ ; $d$ étant par ailleurs un diviseur de $p-1$, on a l'égalité $k \wedge (p-1) = p-1$, d'où $k \mid p-1$.

*Seconde méthode (séries génératrices).*

On part de la factorisation $X^{p-1} - 1 = \prod_{\lambda\in\mathbb{F}_p^*} (X - \lambda)$, exprimant que tout élément $\lambda$ de $\mathbb{F}_p^*$ vérifie $\lambda^{p-1} = 1$ (PTF). On va en prendre la dérivée logarithmique, puis utiliser le développement en série formelle $\frac{1}{1-X} = 1 + X + X^2 + ....$ On va d'abord faire apparaître du $1 - (*)$ pour ne pas s'embêter avec les signes.

En regardant le produit des racines de $X^{p-1} - 1$, on récupère $-1 = \prod_{\lambda\in\mathbb{F}_p^*} (-\lambda)$, d'où $\prod_{\lambda\in\mathbb{F}_p^*} \lambda = (-1)^p$, puis

$$1 - X^{p-1} = -\prod_{\lambda\in\mathbb{F}_p^*} (X - \lambda) = -\prod_{\lambda\in\mathbb{F}_p^*} \lambda \prod_{\lambda\in\mathbb{F}_p^*} \left(\frac{X}{\lambda} - 1\right) = (-1)^{p-1} \prod_{\lambda\in\mathbb{F}_p^*} (\lambda X - 1) = \prod_{\lambda\in\mathbb{F}_p^*} (1 - \lambda X)$$

[3] petit théorème de Fermat

(pour l'avant-dernière égalité, on a dit que l'application $\lambda \mapsto \frac{1}{\lambda}$ était une bijection du groupe $\mathbb{F}_p^*$). On prend maintenant la dérivée logarithmique :

$$\frac{-(p-1)X^{p-2}}{1-X^{p-1}} = \sum_{\lambda\in\mathbb{F}_p^*} \frac{-\lambda}{1-\lambda X} \implies -X^{p-2}\sum_{i\geq 0}\left(X^{p-1}\right)^i = \sum_{\lambda\in\mathbb{F}_p^*}\lambda\sum_{i\geq 0}(\lambda X)^i$$

$$\implies -X^{p-1}\sum_{i\geq 0}X^{i(p-1)} = \sum_{i\geq 0}\left(\sum_{\lambda\in\mathbb{F}_p^*}\lambda^{i+1}\right)X^{i+1} \implies \sum_{i\geq 1}-X^{i(p-1)} = \sum_{i\geq 1}S_iX^i.$$

En identifiant les coefficients en $X$, on retrouve le même résultat que précédemment.

**Remarque.** Le resultat pourrait s'exprimer à l'aide de la fonction caractéristique de $\mathbb{N}$ :

$$\forall k \geq 1,\ S_k = -\chi_{\mathbb{N}}\left(\frac{k}{p-1}\right).$$

# 4 Loi de réciprocité quadratique par le calcul des sommes de Gauss

On se place dans le corps $\mathbb{F}_p$. On rappelle que le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique.
On s'intéresse à la question suivante : un entier $a$ donné est-il un carré modulo un multiple de $p$ ?
On définit pour cela le *symbole de Legendre*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ si } a \text{ est nul modulo } p \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}.$$

*Soit* $x \in \mathbb{F}_p^*$. *Montrer que* $\begin{cases} x \text{ est un carré dans } \mathbb{F}_p^* \text{ ssi } x^{\frac{p-1}{2}} = 1 \\ x \text{ n'est pas un carré dans } \mathbb{F}_p^* \text{ ssi } x^{\frac{p-1}{2}} = -1 \end{cases}$.
*En déduire les relations* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ *et* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Ainsi, pour calculer $\left(\frac{a}{p}\right)$, il suffit de le connaitre pour $a$ premier. On laissera de côté le cas $a = 2$ de côté pour l'exercice[4].

Soient $p$ et $q$ deux nombres premiers impairs distincts. On cherche un rapport entre $\left(\frac{q}{p}\right)$ et $\left(\frac{p}{q}\right)$. Pour cela, de la même manière que l'on introduit dans $\mathbb{R}$ un nombre $i$ imaginaire qui engendre les toutes les racines du polynôme $X^4-1$ (on agrandit $\mathbb{R}$ et tombe sur $\mathbb{C}$), on va rajouter à $\mathbb{F}_q$ un élément $\xi$ qui engendre les racines de $X^p-1$ (cela revient à construire un corps $K$ de décomposition du polynôme $X^p-1$ sur $\mathbb{F}_q$), et on considère la somme dite *de Gauss* :

$$G = \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)\xi^a$$

(qui est un élément du gros corps $K$).

*Montrer que* $G^2 = \left(\frac{-1}{p}\right)p$, *puis que* $G^q = \left(\frac{q}{p}\right)G$, *et en déduire la loi de réciprocité quadratique :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

*Application :* 11 *est-il un carré modulo* 509 *?*

**Solution proposée.**
On a toujours $x^{\frac{p-1}{2}} = \pm 1$ car le carré vaut 1 (PTF).

[4] On peut calculer $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ pour $p$ premier.

Si $x = c^2$ est un carré, alors $x^{\frac{p-1}{2}} = c^{2\frac{p-1}{2}} = c^{p-1} = 1$ par le PTF.

Si $x^{\frac{p-1}{2}} = 1$, écrivons $x = g^k$ où $g$ est un générateur de $\mathbb{F}_p^*$. On a alors $g^{k\frac{p-1}{2}} = 1$, donc l'ordre $p-1$ du générateur $g$ doit diviser $k\frac{p-1}{2}$, disons $k\frac{p-1}{2} = l\,(p-1)$. Ceci implique $\frac{k}{2} = l$, d'où $k$ pair et $x = g^k = \left(g^{\frac{k}{2}}\right)^2$ carré.

On en déduit que le symbole de Legendre se calcule explicitement par $\left(\frac{m}{p}\right) = m^{\frac{p-1}{2}}$, d'où sa multiplicativité et le calcul de $\left(\frac{-1}{p}\right)$.

Calculons à présent les puissances de la somme de Gauss $G$ introduite. On vérifie tout d'abord que $G$ est bien définie : en effet, si $a \in \mathbb{F}_p$, la puissance $\xi^a$ ne dépend pas du représentant $a$ modulo $p$ choisi vu que $\xi^p = 1$. Avanti ! On multidistribue le carré, puis on somme à puissance de $\xi$ constante :

$$G^2 = \left(\sum_{a\in\mathbb{F}_p^*}\left(\frac{a}{p}\right)\xi^a\right)^2 = \sum_{a\neq 0}\left(\frac{a}{p}\right)\xi^a\sum_{b\neq 0}\left(\frac{b}{p}\right)\xi^b = \sum_{a,b\neq 0}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\xi^{a+b} = \sum_{c\in\mathbb{F}_p}\left(\sum_{\substack{a+b=c\\ a,b\neq 0}}\left(\frac{ab}{p}\right)\right)\xi^c.$$

On élimine à présent une variable parmi $a$ et $b$, mettons $b$, puis on homogénéise le $ab$ dans le $\left(\frac{ab}{p}\right)$ :

$$= \sum_c\left(\sum_{a\neq 0,c}\left(\frac{a\,(c-a)}{p}\right)\right)\xi^c = \sum_c\left(\sum_{a\neq 0,c}\underbrace{\left(\frac{a^2}{p}\right)}_{=1}\left(\frac{\frac{a(c-a)}{a^2}}{p}\right)\right)\xi^c = \sum_c\left(\sum_{a\neq 0,c}\left(\frac{\frac{c}{a}-1}{p}\right)\right)\xi^c.$$

Le changement de variables $d = \frac{c}{a} - 1$ nous tend les bras et pour $c \neq 0$ les conditions de sommation $a \neq 0, c$ deviennent plus simplement $d \neq 0, 1$ (il n'y a plus de $c$, ce qui permet de sortir le $\xi^c$) :

$$= \sum_{a\neq 0}\left(\frac{-1}{p}\right) + \sum_{c\neq 0}\left(\sum_{a\neq 0,c}\left(\frac{-1}{p}\right)\left(\frac{1-\frac{c}{a}}{p}\right)\right)\xi^c = (p-1)\left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right)\sum_{c\neq 0}\left(\sum_{d\neq 0,1}\left(\frac{d}{p}\right)\right)\xi^c.$$

Pour calculer $\sum_{d\neq 0,1}\left(\frac{d}{p}\right)$, il convient de remarquer que $\mathbb{F}_p^*$ contient exactement autant de carrés que de non-carrés : considérer le morphisme $\left\{\begin{array}{ccc}\mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2\end{array}\right.$ d'image les carrés et de noyau $\{\pm 1\}$ (qui est bien de cardinal 2 car $p$, supposé impair, est distinct de 2 et par conséquent $1 \neq -1$). Ainsi, $\sum_{d\neq 0,1}\left(\frac{d}{p}\right)$ compte tous les carrés avec un 1 (sauf $d = 1$) et tous les non-carrés avec un $-1$. Il en résulte que $\sum_{d\neq 0,1}\left(\frac{d}{p}\right) = -1$. Finalement :

$$G^2 = \left(\frac{-1}{p}\right)\left(p - 1 + \sum_{c\neq 0} -\xi^c\right).$$

Pour obtenir la somme $\sum_c \xi^c$, il suffit de dire qu'elle vaut le terme en $X^{p-1}$ dans le polynôme $X^p - 1 = \prod_{i=1}^p\left(X - \xi^i\right)$, i.e. 0. On en tire $\sum_{c\neq 0}\xi^c = -1$, d'où

$$G^2 = \left(\frac{-1}{p}\right)(p - 1 + 1) = p\left(\frac{-1}{p}\right).$$

Le calcul de $G^q$ sera moins douloureux. En effet, la relation $q \times 1 = 0$ reste valable dans le gros corps $K$, donc l'élévation à la puissance $q$ reste un morphisme aditif. Comme de plus $q$ est impair, les symboles de Legendre sont inchangés par élévation à la puissance $q$. Ceci étant dit, on peut écrire

$$\begin{aligned} G^q &= \left(\sum_{a\neq 0}\left(\frac{a}{p}\right)\xi^a\right)^q = \sum_{a\neq 0}\left(\frac{a}{p}\right)^q\xi^{qa} = \sum_{a\neq 0}\left(\frac{a}{p}\right)\xi^{qa} = \sum_{b\neq 0}\left(\frac{\frac{b}{q}}{p}\right)\xi^b = \sum_{b\neq 0}\underbrace{\left(\frac{\frac{1}{q^2}}{p}\right)}_{=1}\left(\frac{bq}{p}\right)\xi^b \\ &= \sum_{b\neq 0}\left(\frac{b}{p}\right)\left(\frac{q}{p}\right)\xi^b = \left(\frac{q}{p}\right)\sum_{b\neq 0}\left(\frac{b}{p}\right)\xi^b = \left(\frac{q}{p}\right)G. \end{aligned}$$

Puisque $G^2 = p\left(\frac{-1}{p}\right)$ est non nul (car $p \neq q$), on peut simplifier par $G$ et obtenir

$$G^{q-1} = \left(\frac{q}{p}\right).$$

En élevant la première relation trouvée $G^2 = p\left(\frac{-1}{p}\right) = p\,(-1)^{\frac{p-1}{2}}$ à la puissance $\frac{q-1}{2}$, on trouve

$$G^{q-1} = p^{\frac{q-1}{2}}\,(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Le résultat s'obtient en comparant les deux valeurs de $G^{q-1}$.

Pour l'application, on calcule le symbole de Legendre

$$\begin{aligned}\left(\frac{11}{509}\right) &= (-1)^{5\times 254}\left(\frac{509}{11}\right) = \left(\frac{46\times 11+3}{11}\right) = \left(\frac{3}{11}\right) = (-1)^{5\times 1}\left(\frac{11}{3}\right)\\ &= -\left(\frac{3\times 4-1}{3}\right) = -\left(\frac{-1}{3}\right) = -\,(-1)^{\frac{3-1}{2}} = 1,\end{aligned}$$

donc 11 est bien un carré modulo 509.

# 5 Groupes, arithmétique & corps fini

*Soit $p$ un premier et $(a_n)_{n\geq 0}$ la suite définie par* $\begin{cases} a_0 = 2 \\ a_{n+1} = 2a_n^2 - 1 \end{cases}$.

*Montrer l'implication*

$$p \mid a_n \implies 2^{n+3} \mid p^2 - 1.$$

**Solution proposée.**

Soit $n$ tel que $p \mid a_n$.

Pour conclure, il suffit d'après le théorème de Lagrange de trouver un élément d'ordre $2^{n+3}$ dans un groupe d'ordre $p^2-1$, par exemple le groupe multiplicatif $\mathbb{F}_{p^2}^*$ du corps fini à $p^2$ éléments.

Pour démarrer, vue la formule de récurrence définissant $a_{k+1}$, on a envie de poser $a_k = \cos\theta_k$ pour un certain $\theta_k$ (ce afin d'avoir $\theta_{k+1} = 2\theta_k$), puis $c_k = e^{i\theta_k} = c_0^{2^k}$ qui se prête bien au calcul des puissances. Alors, pour peu qu'il soit légitime de se placer dans $\mathbb{F}_p$, puisque $\cos\theta_n = 0$, on aura $\sin\theta_n = \pm 1$, d'où $c_n = \pm i$ et $c_n^2 = -1$, ce qui montera que l'ordre de $c_n$ est $2^{n+2}$, d'où $2^{n+2} \mid p-1$. Pour conclure, il suffit de considérer une racine carrée $c_{-1}$ de $c_0 = \pm i$, de sorte que $c_{-1}$ sera d'ordre $2^{n+3}$ dans un groupe d'ordre divisant $p^2-1$, *CQFD.*

Comment rendre les idées du paragraphe précédentes rigoureuses ? Si l'on veut rester dans $\mathbb{F}_p$ pour pouvoir appliquer Lagrange, on ne peut plus passer par les $\theta_k$. Tentons de récupérer les $b_k := \sin\theta_k$. Vue la formule de duplication du sinus, il est naturel de poser $b_{k+1} = 2a_kb_k$. Vue la relation souhaitée $a_k^2 + b_k^2 = 1$, on doit avoir $b_0^2 = -1$, *i. e.* $b_0$ racine de $-1$. Admettons pour le moment qu'une telle racine existe dans $\mathbb{F}_p$. On peut alors poser $b_0 = i$, ce qui définit entièrement la suite $(b_k)$, puis on peut récupérer $c_k := a_k + ib_k$.

Si l'on regarde bien le raisonnement heuristique ci-dessus

$$a_n \equiv 0 \implies b_n \equiv \pm 1 \implies c_n \equiv \pm i \implies c_0^{2^{n+1}} = -1 \implies c_0 \text{ d'ordre } 2^{n+2},$$

on a besoin de deux ingrédients : les relations $a_n^2 + b_n^2 = 1$ et $c_n = c_0^{2^n}$. On vérifie alors que $a_k^2 + b_k^2 = 1$ par récurrence sur $k$ (le cas $k=0$ étant vrai par construction de $b_0$), d'où l'on déduit directement la relation $c_{k+1} = c_k^2$ :

$$\begin{aligned}a_{k+1}^2 + b_{k+1}^2 &= \left(2a_k^2-1\right)^2 + (2a_kb_k)^2 = 4a_k^4 - 4a_k^2 + 1 + 4a_k^2\left(1-a_k^2\right) = 1,\\ (a_k+ib_k)^2 &= a_k^2 - b_k^2 + 2ia_kb_k = \left(2a_k^2-1\right) + ib_{k+1} = c_{k+1},\ \textit{CQFD.}\end{aligned}$$

Il reste deux problèmes : extraire une racine carrée $i$ de $-1$ puis extraire une racine carrée de $c_0 = 2+ii = 3$.

Pour le premier, on va rajoute à $\mathbb{F}_p$ une racine $i$ de $-1$ en se plaçant dans l'algèbre

$$\mathbb{F}_p[i] := {}^{\mathbb{F}_p[X]}\!\diagup_{X^2+1}.$$

Deux cas se présentent : ou bien $-1$ était déjà[5] un carré modulo $p$, auquel cas $\mathbb{F}_p[i]$ est isomorphe à $\mathbb{F}_p$, ou bien ce n'était pas le cas, mais alors $X^2+1$ est irréductible et $\mathbb{F}_p[i]$ est un corps de cardinal $|\mathbb{F}_p|^{\deg\left(X^2+1\right)} = p^2$. Dans les deux cas, $\mathbb{F}_p[i]^*$ est un groupe de cardinal divisant $p^2-1$, ce qui nous suffit pour obtenir $2^{n+2} \mid p^2-1$.

Quant à une éventuelle racine de 3, on ne peut évidemment pas en rajouter une à la main comme on l'a fait pour $-1$ puisque cela modifierait de façon déplaisante[6] notre relation $2^{n+2} \mid p^2-1$. En utilisant encore une fois notre intuition complexe où la donnée d'un $\sqrt{-1}$ nous permet d'obtenir un $j$ tel que $j^2+j+1=0$ par la formule $j := \frac{-1+\sqrt{3}i}{2}$, on observe réciproquement que la donnée d'un tel $j$ nous donne une racine carrée de 3 en inversant la formule définissant $j$ :

$$\left(\frac{2j+1}{i}\right)^2 = -\left(4j^2+4j+1\right) = -\left(-4+1\right) = 3.$$

Il suffit donc de trouver un tel $j$ dans $\mathbb{F}_p[i]$.

Or, $\mathbb{F}_p[i]$ a $p^2$ élémets, donc est $\mathbb{F}_{p^2}$, corps de rupture de tout polynôme du second degré sans racine sur $F_p$, en particulier $X^2+X+1$, CQFD.

[5] c'est le cas ssi $p \equiv 1$ modulo 4

[6] le corps $\mathbb{F}_p\left[i, \sqrt{3}\right]$ pourrait être de cardinal $p^4$ (au lieu de $p^2$ comme l'on aimerait)