121 (H) Nombres premiers. Applications.

I - Arithmétique dans $\mathbb{Z}$ [Gourdon]

Déf 1 : Un entier relatif a divise un autre entier b si il existe un entier relatif k tel que $b = ka$. On note $a \mid b$.

Déf 2 : Un entier $p \geq 2$ est dit premier si et seulement si ses seuls diviseurs sont $-p, -1, 1$ et p.

Thm 3 : Lemme d'Euclide :
Soient a et b des entiers relatifs et p premier.
Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$

Application 4. Si p est premier et $0 < k < p$, alors $p \mid \binom{p}{k}$.

Thm 5 : Théorème de Bezout
Si $\operatorname{pgcd}(a,b) = 1$, il existe $u, v \in \mathbb{Z}$ tq $ua + vb = 1$.

Prop 6 : Théorème fondamentale de l'arithmétique
Tout entier $n \geq 2$ s'écrit de manière unique à l'ordre près sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où les p_i sont des premiers distincts et les α_i sont des entiers non nuls

Application 7 : Calcul du pgcd et du ppcm
Soient $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\delta_1} \cdots q_m^{\delta_m}$ et $b = p_1^{\beta_1} \cdots p_k^{\beta_k} r_1^{\varepsilon_1} \cdots r_m^{\varepsilon_m}$
où $q_i \neq r_j$ pour tout i et j.
Alors : • $\operatorname{pgcd}(a,b) = p_1^{\inf(\alpha_1, \beta_1)} \cdots p_k^{\inf(\alpha_k, \beta_k)}$

• $\operatorname{ppcm}(a,b) = p_1^{\sup(\alpha_1,\beta_1)} \cdots p_k^{\sup(\alpha_k,\beta_k)} \times q_1^{\delta_1} \cdots q_m^{\delta_m} \times r_1^{\varepsilon_1} \cdots r_m^{\varepsilon_m}$

Déf 8 : Soit $n > 1$. On note $\varphi(n) = \operatorname{Card} \{ k \in \{1, \dots, n\} \mid \operatorname{pgcd}(n,k) = 1 \}$
On nomme indicatrice d'Euler la fonction φ.

Prop 9 : Soient n et m des entiers premiers entre eux ;
$\varphi(nm) = \varphi(n)\,\varphi(m)$

Prop 10 : Soient p premier et $\alpha \in \mathbb{N}^*$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1}$.

Répartition des nombres premiers

Prop 11 : Il existe une infinité des nombres premiers

Prop 12 : Il n'existe pas de polynôme P non constant tel que $P(n)$ soit premier pour n assez grand.

Thm 13 : Théorème de la progression arithmétique de Dirichlet (admis)
Pour tout entiers a, b premiers entre eux il existe une infinité de nombres premiers de la forme $ak + b$ avec $k \in \mathbb{N}$.

Thm 14 : Théorème des nombres premiers
Notons $\pi(n)$ le nombre de nombres premiers inférieur à n.
$\pi(n) \sim \dfrac{n}{\ln n}$

II - Application à la théorie des groupes [Perrin]

Déf 15 : Un groupe fini est dit p-groupe si et seulement si l'ordre du groupe est une puissance de p.

Déf 16 : Soient G un groupe d'ordre n et p un diviseur premier de n.
Soient $\alpha \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ tels que $n = p^\alpha m$ et $p \nmid m$.
Un p-sous-groupe de Sylow de G est un sous-groupe de cardinal p^α.

Prop 17 : Dire que P est un p-sous-groupe de Sylow de G signifie :
- que P est un p-groupe
- que l'indice $(G : P)$ est premier à p.

Thm 18 : Soient G un groupe d'ordre n et p un diviseur premier de n. Il existe un p-sous-groupe de Sylow.

Thm 19. Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$.
Soit k le nombre de p-sous-groupe de Sylow de G.

- Si H, un sous groupe de G, est un p-groupe, il existe un p-Sylow contenant H.
- Les p-Sylow sont conjugués (et donc $k \mid p^\alpha m$)
- $k \equiv 1 \pmod p$ (et donc $k \mid m$)

Corollaire 20 : Soit S un p-Sylow de G.
S sous-groupe distingué ssi S est l'unique p-Sylow de G
ssi $k = 1$

Application 21 : Prouver qu'un groupe n'est simple en exhibant un p-Sylow distingué.

Ex 22 : Un groupe d'ordre 63 contient un 7-Sylow distingué et donc n'est pas simple

III Corps finis [Perrin]

L'anneau $\mathbb{Z}/_n\mathbb{Z}$

Thm 23 : Un élément k de l'anneau $\mathbb{Z}/_n\mathbb{Z}$ est inversible ssi $\mathrm{pgcd}(k,n) = 1$.

Rq : Cela découle directement du théorème de Bezout. D'ailleurs, l'algorithme d'Euclide étendu, qui permet de calculer les coefficients de Bezout, permet de calculer la valeur de l'inverse.

Corollaire 24 : $\mathbb{Z}/_{n\mathbb{Z}}$ est un corps ssi n est premier.

Prop 25 : Le cardinal des inversibles de $\mathbb{Z}/_{n\mathbb{Z}}$ est $\varphi(n)$.

Corollaire 26 : Théorème d'Euler
Soient n et k premiers entre eux.
$k^{\varphi(n)} \equiv 1 \pmod n$

Propriétés de bases des corps finis

Déf 27 : Soit K un corps et $\varphi : \mathbb{Z} \to K$, $n \mapsto n.1$
$\mathrm{Ker}\,\varphi$ est un idéal de $\mathbb{Z}$, donc $\mathrm{Ker}\,\varphi = c\mathbb{Z}$.
Ce nombre c est appelé caractéristique de K.

Prop 28 : La caractéristique est soit 0, soit un nombre premier.

Thm 29 : Soient p premier et $n \in \mathbb{N}^*$, $q = p^n$.
Il existe un corps à q éléments : c'est le corps de décomposition de $X^q - X$. Ce corps est unique à isomorphisme près.

Déf 30 : Soit un corps K de caractéristique $c > 0$.
On nomme morphisme de Frobenius le morphisme :
$F : K \to K$, $x \mapsto x^c$

Prop 31 : Si K est fini, F est un automorphisme

Thm 32 : Le groupe $\mathbb{F}_q^*$ est cyclique.

Carrés dans $\mathbb{F}_q$

Prop 33 : En caractéristique 2, tous les éléments sont des carrés.
On se place en caractéristique supérieur à 2 pour la suite.

Thm 34 : x est un carré dans $\mathbb{F}_q$ ssi $x^{\frac{q-1}{2}} = 1$

Corollaire 35 : -1 est un carré dans $\mathbb{F}_q$ ssi $q \equiv 1 \ [4]$

Thm 36 : Théorème des deux carrés [DEV]

Un nombre premier impair p est somme de deux carrés si et seulement si $p \equiv 1 [4]$

IV Tests de primalité [Cohen]

Algorithme naïf

On cherche à savoir si un entier N est premier.

On tente alors la division euclidienne de N par tous les entiers compris entre 2 et $\sqrt{N}$.

Si l'un d'eux divise N, N est composé, sinon N est premier

Complexité : $O(\sqrt{N})$ (Si l'on compte les divisions en temps constant)

Pocklington - Lehmer [DEV]

Test déterministe permettant de décider la primalité de N à partir d'une décomposition partielle de N-1

Miller - Rabin.

Soit $\mathcal{C}(a, N)$ la condition suivante :

" Notons $N-1 = 2^s q$, $a^q \equiv 1 \ [N]$ ou il existe $0 \leq r < s$ tq $a^{2^r q} \equiv -1 \ [N]$ "

Si N est premier, pour tout a, $\mathcal{C}(a, N)$ est vérifiée.

Si N n'est pas premier, au moins trois quart des entier a entre 1 et $n-1$ ne vérifient pas $\mathcal{C}(a, N)$.

Donc on teste $\mathcal{C}(a, N)$ pour une suite aléatoire de valeurs de a, et si $\mathcal{C}(a, N)$ est toujours vérifié, on dit que l'on est "presque sûr" que N est premier.

Application à la cryptographie : RSA.

- On choisit des premiers p et q grands. Soit $n = pq$
- On souhaite transmettre un message $M < n$ en le chiffrant par C
- On choisit e premier avec $\varphi(n)$.
- On calcule l'inverse de e dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$, noté d.
- Chiffrement : $C = M^e$
- Déchiffrement : $M = C^d$

Le théorème des 2 carrés

On pose $\Sigma = \{n \in \mathbb{N},\ n = a^2+b^2,\ a,b \in \mathbb{N}\}$.

On veut montrer que, pour p premier impair, $p \in \Sigma \iff p \equiv 1[4]$.

L'idée est ici de démontrer ce théorème à partir des entiers de Gauss. Étudions donc d'abord l'anneau $\mathbb{Z}[i]$

I] $\mathbb{Z}[i]$

On définit l'anneau des entiers de Gauss, $\mathbb{Z}[i]$, par $\mathbb{Z}[i] = \{a+ib \in \mathbb{C},\ a,b \in \mathbb{Z}\}$

C'est un anneau inclus dans $\mathbb{C}$, donc intègre. De plus on peut y définir l'automorphisme suivant : $\sigma : \begin{cases} \mathbb{Z}[i] \to \mathbb{Z}[i] \\ a+ib \mapsto a-ib \end{cases}$, appelé la conjugaison. On notera alors $\sigma(z) = \bar{z}$

Définissons dès lors $N : \begin{array}{l} \mathbb{Z}[i] \to \mathbb{N} \\ z = a+ib \mapsto z\bar{z} = a^2+b^2 \end{array}$

N est multiplicative ($N(zz') = N(z)N(z')$)

Proposition 1 : $\mathbb{Z}[i]$ possède 4 éléments inversibles : $\{1, i, -1, -i\}$.

// si $z \in \mathbb{Z}[i]^*$, alors, $N(zz^{-1}) = N(z)N(z^{-1}) = N(1) = 1$. donc $N(z) = N(z^{-1}) = 1$.

Donc $a^2+b^2 = 1 \Rightarrow (a=0$ et $|b|=1)$ ou $(|a|=1$ et $b=0)$ d'où le résultat

Comme N est multiplicative, Σ, qui est donc l'ensemble des "normes" d'éléments de $\mathbb{Z}[i]$, est stable par multiplication

Proposition 2 : $\mathbb{Z}[i]$ est un anneau euclidien

// Soit $z, t \in \mathbb{Z}[i] \setminus \{0\}$, on a $\frac{z}{t} = x+iy$, $x,y \in \mathbb{R}$.

Posons $q = a+ib$, avec $|a-x| \leq 1/2$ et $|b-y| \leq 1/2$.

Alors $\left|\frac{z}{t}-q\right| \leq \frac{\sqrt{2}}{2} < 1$

Posons $r = z - qt$.

$r \in \mathbb{Z}[i]$ et $r = t\left[z/t - q\right]$ d'où $|r| = |t| \cdot |z/t - q| \leq |t|$, donc $N(r) < N(t)$.

On a donc bien établi une division euclidienne de z par t, d'où le résultat.

Maintenant qu'on a établi la base de notre travail, démontrons le théorème proprement dit.

On aura besoin du lemme suivant

__Lemme 3__ $p \in \Sigma \Leftrightarrow p$ non irréductible dans $\mathbb{Z}[i]$.

$\Rightarrow$ Si $p = a^2 + b^2 = (a+ib)(a-ib)$, avec $a, b \neq 0$, alors $\begin{cases} a+ib \notin \mathbb{Z}[i]^* \\ a-ib \notin \mathbb{Z}[i]^* \end{cases}$ donc p n'est pas irréductible

$\Leftarrow$ si $p = zz'$, avec z, z' non inversibles (donc $N(z) \neq 1$ et $N(z') \neq 1$.

$N(p) = N(z)N(z') = p^2$. Or p est premier, donc nécessairement, $p = N(z)$ d'où le résultat

Démo du théorème des 2 carrés.

On a une norme N, et $\mathbb{Z}[i]$ est euclidien pour N, donc factoriel

Alors p non irréductible dans $\mathbb{Z}[i] \Leftrightarrow (p)$ n'est pas premier

$\Leftrightarrow \mathbb{Z}[i]/(p)$ non intègre.

Or $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ donc $\mathbb{Z}[i]/(p) \simeq \left(\mathbb{Z}[X]/(p)\right)/(X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$.

D'où

p non irréductible dans $\mathbb{Z}[i]$ $\Leftrightarrow (X^2+1)$ non irréductible dans $\mathbb{F}_p[X]$.

$\Leftrightarrow X^2+1$ admet une racine dans $\mathbb{F}_p$.

$\Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$.

On veut montrer $p \in \Sigma \Leftrightarrow p \equiv 1[4]$

Il suffit alors de montrer que $p \equiv 1[4] \Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$.

Or, (-1) est un carré dans $\mathbb{F}_p \Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1[4]$

__cqfd__

Remarque : $2 = 1^2 + 1^2$, donc $2 \in \Sigma$.

On a donc caractérisé un nombre premier p concernant son appartenance à Σ.

Peut-on en faire de même pour n'importe quel entier $n \in \mathbb{N}$.

Corollaire 4 : Soit $n \in \mathbb{N}$, $n = \prod p_i^{\nu_{p_i}}$, avec ν_{p_i} multiplicité de p_i dans n.

alors $n \in \Sigma \iff \forall i \mid p_i \equiv 3[4] \Rightarrow 2 \mid \nu_i$.

Demonstration.

$\boxed{\Leftarrow}$ On décompose n de la manière suivante

$$n = \prod_{i / p \equiv 3[4]} p_i^{\nu_i} \prod_{i/p \not\equiv 3[4]} p_i^{\nu_i} = \underbrace{\left(\prod_{i/p\equiv 3[4]} p_i^{\nu_i/2} \right)^2}_{\alpha} \underbrace{\left(\prod_{i/p \not\equiv 3[4]} p_i^{\nu_i} \right)}_{\beta}$$

α est un carré parfait, donc appartient à Σ.

et $\beta \in \Sigma$ par stabilité de Σ pour la multiplication

en effet, si $p \not\equiv 3[4]$, alors $p = 2$ ou $p \equiv 1[4]$, donc $p \in \Sigma$.

$\boxed{\Rightarrow}$ Soit $n = a^2 + b^2$, quitte à considérer $\frac{n}{(a \wedge b)^2}$, on peut considérer que $a \wedge b = 1$.

Soit $p \in \mathcal{P}$ divisant n. $a^2 + b^2 \equiv 0[p]$.

p ne divise pas a, sinon, p diviserait $n - a^2 = b^2$, donc p diviserait b et a, donc $a \wedge b$ serait différent de 1. De même, $p \nmid b$.

Donc $(ab^{-1})^2 \equiv -1[p_i]$ et $b \in \mathbb{F}_p^*$ donc, -1 est un carré modulo p.

D'après le thm des 2 carrés, on a donc $p_i = 2$ ou $p_i \equiv 1[4]$.

Donc, si $p_i \equiv 3[4]$ $\nu_i = 0$

Remarque Le cas $d \neq 1$ nous donnera la condition ν_i pair au lieu de $\nu_i = 0$

Le test de Pocklington-Lehmer.

Le but : Trouver un test de primalité ne dépendant pas d'arguments probabilistes. (On notera ici le pgcd de a et b : $(a \wedge b)$.

Proposition 1 : Soit N un nombre entier, et p diviseur premier de $N-1$. Supposons que l'on puisse trouver un entier a_p tel que $a_p^{N-1} \equiv 1 [N]$, et que $\left(a_p^{(N-1)/p} - 1\right) \wedge N = 1$. Alors tout diviseur d de N est congru à 1 modulo p^{α_p}, p^{α_p} étant la plus grande puissance de p divisant $N-1$.

[redacted]

Demonstration

Il suffit de montrer cela pour n'importe quel diviseur premier de N.

Soit donc d diviseur premier de N.

Comme $a_p^{N-1} \equiv 1 [N]$, a_p est premier avec N (Bezout), et donc a_p est premier avec d, on a $a_p^{d-1} \equiv 1 [d]$

De plus, si $\left(a_p^{(N-1)/p} - 1\right) \wedge N = 1$, alors $a_p^{(N-1)/p} \not\equiv 1 [d]$.

En effet, soit la relation de Bezout entre $a_p^{(N-1)/p} - 1$ et N :

$$A\left[a_p^{(N-1)/p} - 1\right] + BN = 1.$$ Alors, modulo d, on obtient

$$A\left[a_p^{(N-1)/p} - 1\right] \equiv 1 [d],$$ soit A^{-1} inverse de A modulo d., en particulier $A^{-1} \not\equiv 0 [d]$

alors $a_p^{(N-1)/p} \equiv A^{-1} + 1 [d]$ et donc $a_p^{(N-1)/p} \not\equiv 1 [d]$.

Soit donc e l'ordre de a_p modulo d.

$\begin{cases} e \text{ divise } d-1 \\ e \text{ divise } N-1 \end{cases}$, mais e ne divise pas $\frac{N-1}{p}$, donc $p^{\alpha_p} | e | d-1$, avec α_p défini précédemment d'où le résultat.

Cette proposition nous offre donc un test de primalité rapide dès lors que l'on connaît la factorisation de $N-1$, car N est premier si on peut vérifier la proposition 1 pour tout p.

Cependant, puisque factoriser un entier se révèle parfois pénible, exhibons ~~deux~~ corollaires pour lesquel une factorisation partielle est suffisante

---

<u>Corollaire 1</u> : Soit N un entier, que l'on suppose de la forme $1+FU$, avec $\begin{cases} F \wedge U = 1 \\ F \text{ complètement factorisé} \\ F > \sqrt{N} \end{cases}$

Si pour tout p diviseur premier de F, on connaît et on peut exhiber un a_p vérifiant la propriété 1, alors N est premier

Réciproquement si N est premier, tout p divisant $N-1$ possède un tel a_p.

Démonstration.

Supposons les hypothèses du corollaire satisfaites.

La proposition 1 nous affirme alors que tout diviseur de N est congru à 1 modulo F.
Comme $F > \sqrt{N}$. N n'a aucun diviseur premier inférieur à sa racine carré, donc N est premier.

Réciproquement, supposons N premier. et prenons a_p racine primitive modulo N. (un générateur de $(\mathbb{Z}/N\mathbb{Z})^*$.) Comme l'ordre de a_p vaut exactement $N-1$, alors la proposition 1 est vérifié donc on a prouvé notre résultat.

Corollaire 2. Soit $N = FU+1$, avec $\begin{cases} F \wedge U = 1 \\ F \text{ complètement factorisé} \\ \exists b \in \mathbb{N} \left(\forall p \mid U,\ p > b \right) \wedge \left(b.F > \sqrt{N} \right) \end{cases}$

Alors si pour tout p diviseur de F, on exhibe a_p vérifiant la proposition 1 <u>ET</u> a_U tel que $\left(a_U^{N-1} \equiv 1 \,[N]\right)$ et $\left((a_U^F - 1, N) \wedge N\right) = 1$, alors N est premier

Réciproquement si N est premier, de tels a_p et a_U existent toujours

Démo On suit exactement la démo de la proposition 1

Soit d diviseur premier de N;

alors $d \equiv 1[F]$ et, si e est l'ordre de a_q modulo d, $\begin{cases} e \mid d-1 \\ e \mid N-1 \\ e \nmid F. \end{cases}$

Si $(e \wedge U)=1$, alors $e \mid N-1 \Rightarrow e \mid FU \Rightarrow e \mid F$. ce qui contredit l'hypothèse.

donc $\underline{e \wedge U > b}$.

De plus, comme $F \wedge U = 1$, alors $\begin{cases} d \equiv 1[e] \\ d \equiv 1[F] \end{cases} \Rightarrow d \equiv 1 \left[(e \wedge U)F\right]$ donc

$d > b.F$ donc $d > \sqrt{N}$, et donc N n'a aucun

diviseur premier inférieur à sa racine.

d'où N est premier.

Exemple d'application

Nous pouvons trouver un exemple d'application directe, par exemple avec $N = 11351$

avec $N-1 = 2 \cdot 5^2 \cdot 227$.

(on pose $F = 5^2 \times 227$, on prend $\begin{cases} a_5 = 2 \\ a_{227} = 7. \end{cases}$

Application avec les nombres de Fermat $F_n = 2^{2^n} - 1$.

ici, le seul diviseur premier de $F_n - 1$ est 2, donc il suffit de montrer la propriété pour a_2.

Cette version est aussi appelé le test de ~~Lucas-Lehmer~~ Pépin et est énoncé comme ceci

<u>Prop 2</u>: Soit $F_n = 2^{2^n} - 1$ le n-ième nombre de Fermat

Alors F_n est premier si (et seulement si) $3^{(F_n-1)/2} \equiv -1 [F_n]$.

Démo : si $3^{(F_n-1)/2} \equiv -1[F_n]$, alors $3^{F_n-1} \equiv 1[F_n]$, donc l'ordre de 3 dans $(\mathbb{Z}/F_n\mathbb{Z})^*$ divise $F_n - 1$,

mais pas $\frac{F_n-1}{2}$, donc est égal à $F_n - 1$, donc, il existe $F_n - 1$ entiers premiers avec F_n, et

donc F_n est premier.

Reference.- Cohen, A course in Computational Algebraic theory (pour Pocklington-Lehmer)
Perrin, Cours d'Algèbre (pour les 2 carrés).

- C'est quoi le symbole de Legendre ? $\longrightarrow \left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un carré mod } p \\ 0 \text{ si } p \mid a \\ -1 \text{ sinon} \end{cases}$
- Comment on démontre le thm de la progression arithmétique ? / thm des nombres premiers ? $\longrightarrow$ Analyse complexe
- Pourquoi "p irréductible dans $\mathbb{Z}[i]$ ssi (p) n'est pas premier" ? $\longrightarrow \mathbb{Z}[i]$ est factoriel
- $u_0 = 3$, $u_1 = 0$, $u_2 = 2$ et $\forall n \geq 3$, $u_n = u_{n-2} + u_{n-3}$, montrer que si p est premier, $p \mid u_p$ $\Longrightarrow$ Le polynôme caractéristique est $X^3 - X - 1$. On note α, β, γ ses racines.
Alors $\forall n \in \mathbb{N}$, $u_n = a\alpha^n + b\beta^n + c\gamma^n$. On montre par récurrence triple que $a = b = c = 1$. (ou on montre que ça marche sur u_0, u_1 et u_2, et on conclut en disant que deux suites vérifiant la même relation de réc et qui coïncident sur assez de termes sont égales).
On regarde la même suite dans $\mathbb{F}_p$. On a $\forall n \in \mathbb{N}$, $\overline{u_n} = a^n + b^n + c^n$ avec a, b et c les racines dans $\mathbb{F}_p$ de $X^3 - X - 1$.
En particulier $\overline{u_p} = a^p + b^p + c^p$
$= (a + b + c)^p$
$= 0$
car $a + b + c$ est le terme en X^2 de $X^3 - X - 1$.
- La réciproque est-elle vraie ? Si $n \mid u_n$ alors n est premier ? $\longrightarrow$ non, $1 \mid u_1$!
- Montrer que $n \in \mathbb{N}$ est un carré ssi il est un carré dans tous les $\mathbb{Z}/p\mathbb{Z}$. $\rightarrow$ dur :

$\boxed{\Rightarrow}$ Facile.

$\boxed{\Leftarrow}$ Par contraposée, soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ un non carré. $\exists i_0 \in \{1, \dots, k\}$, $\alpha_{i_0} = 1 [2]$.

On cherche p premier tel que $\left(\frac{n}{p}\right) = -1$. Or $\left(\frac{n}{p}\right) = \left(\frac{p_1}{p}\right)^{\alpha_1} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k}$.

Par le théorème chinois(*) on peut trouver p (pas premier a priori) tel que $p = 1 [4]$, $p = 1 [p_i]$ pour $i \neq i_0$ et $p = a [p_{i_0}]$ avec a un non carré modulo p_{i_0}. Le théorème de la progression arithmétique assure qu'on peut trouver une infinité de tels p premier, en particulier un, et il répond à la question.

(*) Si aucun des p_i n'est 2, sinon il faut faire attention.