

Solutions des exercices de la pl. 18

Exercice 1. a) (Résultat cité à propos du crible d'Eratosthène). Si $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ et $n \notin \mathbb{P}$, montrer qu'il a toujours un facteur premier inférieur ou égal à \sqrt{n} .

b) Montrer que si le plus petit facteur premier p d'un nombre n est strictement plus grand que $\sqrt[3]{n}$ alors ou bien n est premier ou bien n est le produit de deux nombres premiers.

Solution 1 a) Soit p_1 le plus petit facteur premier dans la déc. de n . Comme n n'est pas premier $n = p_1 q$ avec $q \geq p_1$, donc $n \geq p_1^2$ i.e. $p_1 \leq \sqrt{n}$.

b) (M1) Par contraposée. La négation de la conclusion est qu'il existe trois nombres p, q, r tous différents de 1 tel que $n = pqr$. SRdG on prend pour p le plus petit diviseur premier de n . Alors $q \geq p$ et $r \geq p$ et donc $n \geq p^3$ ce qui donne la négation de l'hyp.

(M2) Si p est le plus petit facteur premier de n , il vérifie $p > \sqrt[3]{n}$, on considère $m = n/p \in \mathbb{N}$.

On veut montrer que ou bien $m = 1$ ou bien m est premier.

Or $m = \frac{n}{p} < \frac{n}{\sqrt[3]{n}} = n^{2/3}$. Si m n'est pas premier et différent de 1, par le a), il admet un facteur

premier $p_1 \leq m^{1/2}$ donc par l'inég. précédente $p_1 < (n^{2/3})^{1/2} = n^{1/3}$. Donc p_1 est un facteur premier de n inférieur strictement à $n^{1/3}$ *contradiction*.

Exercice 2. a) En adaptant la preuve d'Euclide, et en considérant $A = 4(\prod_{i=1}^n p_i) - 1$ montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 4.

Remarque - Il est aussi vrai, mais cela demande un argument supplémentaire, qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.

b) Adapter encore cette preuve pour montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 6.

Solution 2 a) *Par l'absurde* Supposons que l'ensemble des nombres premiers congrus à -1 modulo 4 est fini : on le note $\{p_1, \dots, p_k\}$ et on prend $N = 4p_1 \dots p_k - 1$.

Avec la forme de N on voit que N est premier avec tous les nombres p_i .

Mais comme $N \equiv -1 [4]$ il admet nécessairement un diviseur premier congru à -1 mod. 4.

(Par l'absurde sinon, si tous les diviseurs premiers de N étaient congrus à 1 mod. 4 (ou 2) le résultat du produit serait 1 ou 2 ou 4 mod. 4 et donc N serait congru à 1 ou 2 ou 4 modulo 4.)

b) *Par l'absurde* Supposons que l'ensemble des nombres premiers congrus à -1 modulo 6 est fini : on le note $\{p_1, \dots, p_k\}$ et on prend $N = 6p_1 \dots p_k - 1$.

Avec la forme de N on voit que N est premier avec tous les nombres p_i .

Or à part 2, les nombres premiers sont impairs donc congrus à 1, 3, -1 modulo 6. En outre un nombre congru à 3 modulo 6 est divisible par 3.

Donc à part 2 et 3 tous les nombres premiers sont congrus à 1 ou à -1 modulo 6.

Mais comme $N \equiv -1 [6]$, on sait que N n'est divisible ni par 2 ni par 3.

Donc tous les diviseurs premiers de N sont congrus à 1 ou -1 modulo 6.

Sous-par-l'absurde si tous les diviseurs premiers de N étaient congrus à 1 modulo 6 on aurait par produit $N \equiv 1 [6]$, ce qui n'est pas vrai.

Donc N admet au moins un diviseur premier congru à -1 modulo 6, mais ceci est une *contradiction* avec le fait que $N \wedge p_i = 1$ pour chaque p_i premier congru à -1 modulo 6.

Exercice 3 (Nombres premiers et divisibilité des binomiaux).

a) Soit $n \in \mathbb{N}^*$. Montrer que $\binom{2n+1}{n} \leq 4^n$.

b) Pour tout $n \in \mathbb{N}$, on note $\mathbb{P}_n = \{p \in \mathbb{P}, p \leq n\}$.

i) Soit $n = 2k + 1$ un entier impair. Justifier que pour tout nombre premier p tel que $k + 2 \leq p \leq 2k + 1$, p divise $\binom{2k+1}{k}$.

ii) En déduire que si on note N le produit des nombres premiers p tels que $k + 2 \leq p \leq 2k + 1$, on a $N \leq \binom{2k+1}{k}$.

c) Déduire de ce qui précède que $\prod_{p \in \mathbb{P}_n} p < 4^n$.

Solution 3 a) Ah cela nous change des exercices sur $\binom{2n}{n}$ qui est l'unique binomial maximal de la ligne $2n$ du triangle.

Ici on a $\binom{2n+1}{n}$ qui est le binomial maximal, mais il a un frère, qui est $\binom{2n+1}{n+1}$, on va regarder les deux ensembles.

L'idée est que $\binom{2n+1}{n} = \binom{2n+1}{n+1}$ et que si l'on somme les deux, $\binom{2n+1}{n} + \binom{2n+1}{n+1}$ reste inférieur à la somme de tous les binomiaux de cette ligne, donc à 2^{2n+1} .

Ainsi $2\binom{2n+1}{n} \leq 2^{2n+1}$, donc $\binom{2n+1}{n} \leq 4^n$.

b) Questions bien guidées

(i) D'abord $\binom{2k+1}{k} = \frac{(2k+1)(2k)\dots(k+2)}{k!}$.

Pour chaque nombre premier $p \in \llbracket k+2, 2k+1 \rrbracket$, p divise $(2k+1)(2k)\dots(k+2)$

En outre $p \wedge (k!) = 1$ puisque p est premier et $p > k$ donc aucun des facteurs de $k!$ ne peut contenir p comme diviseur premier.

Donc en écrivant $(2k+1)(2k)\dots(k+2) = k! \binom{2k+1}{k}$, on a $p | (k!) \binom{2k+1}{k}$ et $p \wedge (k!) = 1$ donc $p | \binom{2k+1}{k}$.

(ii) Notons $N = p_1 \dots p_r$. Par le (i), $p_i | \binom{2k+1}{k}$ pour chaque i et p_1, \dots, p_r sont deux à deux premiers entre eux, donc $N = p_1 \dots p_r | \binom{2k+1}{k}$ en particulier $N \leq \binom{2k+1}{k}$.

c) Là on essaie d'utiliser le b), la récurrence s'impose, encore faut-il comprendre la distinction de cas n pair / n impair.

Notons $P_n = \prod_{p \in \mathbb{P}_n} p$. Notons $H(n) : P_n < 4^n$.

- Initialisation : $P_2 = 2$ et on a donc bien $P_2 < 4^2$ donc $H(2)$ est vraie.

- Hérité : supposons $H(k)$ vrai pour tous les $k \leq n-1$.

Si n est pair alors $P_n = P_{n-1}$ donc $H(n)$ est vraie.

Si n est impair, on l'écrit $n = 2k+1$. Alors en notant N , comme à la question précédente, le produit de tous les nombres premiers entre $k+2$ et $2k+1$, on a : $P_n = P_{2k+1} = N \cdot P_{k+1}$.

Or par Hypothèse de récurrence forte, $P_{k+1} < 4^{k+1}$ et par le b) (ii), $N \leq \binom{2k+1}{k} \leq 4^k$.

Donc $P_n = N \cdot P_{k+1} < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n$.

La récurrence est établie. □

Exercice 4. a) Montrer que pour tout $(a, b) \in (\mathbb{Z}^*)^2$, $a^2 | b^2 \Leftrightarrow a | b$.

b) Montrer que si $a \wedge b = 1$ et $ab = c^n$ (avec a, b, c dans \mathbb{N} , $n \in \mathbb{N}^*$) alors il existe a_1, b_1 tels que $a = a_1^n$ et $b = b_1^n$.

c) Montrer que si a, b, m, n dans \mathbb{N}^* vérifient $a^m = b^n$ et $m \wedge n = 1$ alors $\exists c \in \mathbb{N}^*$ tel que $a = c^n$ et $b = c^m$.

Solution 4 a) Sens \Leftarrow trivial. La récip. avec les v_p qui permettent en fait de raisonner par équivalence.

Rappel : $m | n$ équivaut à : pour tout $p \in \mathbb{P}$, $v_p(m) \leq v_p(n)$.

Donc $a^2 | b^2 \Leftrightarrow \forall p \in \mathbb{P}, v_p(a^2) \leq v_p(b^2) \Leftrightarrow \forall p \in \mathbb{P}, 2v_p(a) \leq 2v_p(b) \Leftrightarrow \forall p \in \mathbb{P}, v_p(a) \leq v_p(b) \Leftrightarrow a | b$. □

b) Par D.F.P. on sait qu'il existe $a_1 \in \mathbb{Z}$ tel que $a = a_1^n$ si, et seulement si, pour tout $p \in \mathbb{P}$, $n | v_p(a)$.

Or par hyp. $ab = c^n$. donc pour tout $p \in \mathbb{P}$, $v_p(ab) = nv_p(c)$ i.e. $n | v_p(a) + v_p(b)$ (*).

Mais comme $a \wedge b = 1$, on sait que pour $p \in \mathbb{P}$, $v_p(a)$ ou $v_p(b)$ est nul.

Donc (*) entraîne que $\forall p \in \mathbb{P}$, $n | v_p(a)$ et $n | v_p(b)$ et la conclusion. □

c) Pour tout p premier : $v_p(a^m) = mv_p(a) = nv_p(b)$. Comme m et n sont premiers entre eux, on a m divise $v_p(b)$ et n divise $v_p(a)$. Mais plus précisément si on écrit $v_p(b) = mk_p$ on a $nmk_p = mv_p(a)$ donc $v_p(a) = nk_p$. On considère maintenant $c = \prod_{p \in \mathbb{P}} p^{k_p}$.

On a $a = c^n$ et $b = c^m$.

Exercice 5. Soit $p \in \mathbb{P}$ et $(a, b) \in \mathbb{N}^2$ tels que $a^2 - b^2 = p$. Déterminer a et b .

Solution 5 Par factorisation : $a^2 - b^2 = p \Leftrightarrow (a-b)(a+b) = p$ (E).

L'équation (E) dit donc que $a-b$ et $a+b$ sont deux diviseurs de p : comme $a+b \geq 0$ et que le produit $(a-b)(a+b)$ est positif, on en déduit aussi que $a-b \geq 0$.

Comme p est premier et que $0 \leq a - b \leq a + b$, on en déduit que $a - b = 1$ et $a + b = p$.

Ceci entraîne en particulier que $2a = p + 1$ et donc que p est *impair*.

Donc l'équation n'a pas de solution si $p = 2$.

Si $p \in \mathbb{P} \setminus \{2\}$ l'équation équivaut alors $a = (p + 1)/2$ et $b = (p - 1)/2$.

Exercice 6. Soit $(a, n) \in (\mathbb{N}^*)^2$. Montrer que si $\sqrt[n]{a} \in \mathbb{Q}$ alors $\sqrt[n]{a} \in \mathbb{N}$.

Solution 6 On note \mathbb{P} l'ensemble des nombres premiers. On utilise le lemme suivant :

Lemme : Soit $(a, n) \in (\mathbb{N}^*)^2$. On a l'équivalence : $\sqrt[n]{a} \in \mathbb{N}$ si, et seulement, si pour tout $p \in \mathbb{P}$, $n|v_p(a)$

Preuve du lemme : Bien sûr $\sqrt[n]{a} \in \mathbb{N} \Leftrightarrow \exists b \in \mathbb{N}, a = b^n$ (*).

Le sens \Rightarrow du lemme est alors évident : si on a (*), et si on fixe un $p \in \mathbb{P}$, en prenant la valuation p -adique dans (*), on a $v_p(a) = nv_p(b)$ donc $n|v_p(a)$.

Sens \Leftarrow : on suppose que pour tout $p \in \mathbb{P}$, $n|v_p(a)$. On veut fabriquer un $b \in \mathbb{N}$ tel que $a = b^n$.

On considère la D.F.P. de a qui s'écrit $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

L'hypothèse est alors que pour tout $i \in \llbracket 1, r \rrbracket$, $n|\alpha_i$, ce qu'on note $\alpha_i = n\beta_i$ avec $\beta_i \in \mathbb{N}$.

On pose alors $b = p_1^{\beta_1} \dots p_r^{\beta_r} \in \mathbb{N}$. On a bien $b^n = a$. □

Application du lemme à l'exercice :

Soit $a \in \mathbb{N}^*$ tel que $\sqrt[n]{a} \in \mathbb{Q}$. Autrement dit, il existe un couple $(m, d) \in (\mathbb{N}^*)^2$ tel que $\sqrt[n]{a} = \frac{m}{d}$.

En prenant la puissance n de cette égalité, on a $d^n = am^n$ (†).

Deux rédactions de la même idée pour conclure :

(R1) : Par l'absurde, supposons que $\sqrt[n]{a} \notin \mathbb{N}$. Alors par le lemme, il existe un nombre premier $p \in \mathbb{P}$ tel que $v_p(a)$ n'est pas divisible par n .

Or en prenant la valuation p -adique dans (†), on a $nv_p(d) = v_p(a) + nv_p(m)$ ce qui prouve que n divise $v_p(a)$, *contradiction*.

(R2) : Pour tout $p \in \mathbb{P}$, on déduit de (†) que $nv_p(d) = v_p(a) + nv_p(m)$ et donc que $n|v_p(a)$ et par le lemme on conclut que $\sqrt[n]{a} \in \mathbb{N}$.

Exercice 7. Montrer que

- $\log_{10}(2)$ est irrationnel,
- plus généralement, pour tout entier $n \geq 2$, $\log_{10}(n)$ est soit entier, soit irrationnel.
- Pour quelle valeurs de m , la méthode précédente s'applique-t-elle pour montrer que $\log_m(n)$ est entier ou irrationnel?

Solution 7 a) *par l'absurde* si $\log_{10}(2) \in \mathbb{Q}$ alors $\log_{10}(2) = \frac{a}{b}$ avec $(a, b) \in (\mathbb{N}^*)^2$ (on sait que $\log_{10}(2) > 0$). On rappelle que la fonction réciproque de \log_{10} est $x \mapsto 10^x$.

Ainsi on a : $2 = 10^{\frac{a}{b}}$ donc $2^b = 10^a = 2^a 5^a$ ce qui pour a non nul contredit l'unicité de la décomposition en facteurs premiers car les deux membres n'ont pas la même valuation 5-adique.

Donc $\log_{10}(2) \notin \mathbb{Q}$.

b) Généralisation : si $n \in \mathbb{N}_{\geq 2}$ et si l'absurde $\log_{10}(n) = \frac{a}{b}$ avec $(a, b) \in (\mathbb{N}^*)^2$, on a de même $n = 10^{a/b}$ donc $n^b = 10^a$ ou encore $n^b = 2^a 5^a$. Cette égalité donne $bv_2(n) = a$ et $bv_5(n) = a$ en particulier $b|a$.

Or, on peut supposer $a \wedge b = 1$ (écriture irréductible de la fraction initiale) donc avec $b|a$ on déduit que $b = 1$. Donc $n = 10^a$ et dans ce cas, $\log_{10}(n) = a$ un entier.

On vient bien de montrer que si $\log_{10}(n)$ est rationnel alors $\log_{10}(n)$ est un entier, ce qui montre bien l'affirmation de l'énoncé : $\log_{10}(n)$ est soit entier, soit irrationnel.

c) (i) Soit $m \geq 2$ un entier, supposons que $n \geq 2$, $\log_m(n) \in \mathbb{Q}$.

Alors $\log_m(n) = a/b$ avec $(a, b) \in (\mathbb{N}^*)^2$, $a \wedge b = 1$ alors $n = m^{a/b}$ donc $n^b = m^a$.

Donc pour tout $p \in \mathbb{P}$, $bv_p(n) = av_p(m)$ donc $b|av_p(m)$

Si on a un $p \in \mathbb{P}$ tel que $v_p(m) = 1$ alors on en déduit de même que $b|a$ et donc que $b = 1$.

Ainsi $n = m^a$ et $\log_m(n) \in \mathbb{N}$.

Conclusion : on vient de trouver une condition suffisante sur m qui permet de faire la « même preuve qu'au b) » : s'il existe un p premier tel que $v_p(m) = 1$ alors pour tout $n \in \mathbb{N}_{\geq 2}$, $\log_m(n)$ est soit entier, soit irrationnel.

Exercice 8. Je suis un carré parfait à 4 chiffres dont chacun des chiffres est inférieur à 6. En rajoutant 3 à chacun de mes chiffres, on obtient encore un carré parfait, qui suis-je ?

Solution 8 Notons x le nombre mystère, on sait que $x = a^2$ avec $a \in \mathbb{N}$.

L'énoncé dit que $x + 3333 = b^2$ avec $b \in \mathbb{N}$, donc $b^2 - a^2 = 3333$. Donc $(b - a)(b + a) = 3333$.

Ceci ressemble à l'exercice 5, en un peu plus fin car 3333 n'est pas premier, mais a pour D.F.P. : $3333 = 3 \times 11 \times 101$.

L'ensemble $\Delta(3333)$ des diviseurs de 3333 est donc formé de huit éléments :

$$\Delta(3333) = \{3^\alpha \times 11^\beta \times 101^\gamma, (\alpha, \beta, \gamma) \in \llbracket 0, 1 \rrbracket^3\}$$

ou plus explicitement dans l'ordre :

$$\Delta(3333) = \{1, 3, 11, 33, 101, 303, 1111, 3333\}$$

Attention : Il faut tester les quatre décompositions possibles de 3333 en un produit $m \times n$ avec $m \geq n$ pour avoir toutes les valeurs possibles de $m = b + a$ et $n = b - a$ et finalement donc de $a = (m - n)/2$

$$3333 = 3333 \times 1 \quad \text{alors} \quad a = 1666 \quad (1)$$

$$= 1111 \times 3 \quad \text{alors} \quad a = 554 \quad (2)$$

$$= 303 \times 11 \quad \text{alors} \quad a = 146 \quad (3)$$

$$= 101 \times 33 \quad \text{alors} \quad a = 34 \quad (4)$$

$$(5)$$

Or parmi ces quatre valeurs de a , la seule qui donne un carré à 4 chiffres est $a = 34$. Le nombre mystère est donc $x = 1156$.

Exercice 9 (Mersenne et parfait). Soient $n \geq 2$ et $a \geq 2$ des entiers.

a) Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier. On appelle nombre de Mersenne les $M_p = 2^p - 1$ avec p premier.

Culturel : ces nombres sont importants car on dispose d'un bon test pour savoir si M_p est premier. Le plus grand nombre premier connu est un nombre de Mersenne : en 2018 $M_{82589933}$.

b) Un nombre entier naturel est dit parfait s'il est la somme de ses diviseurs dans \mathbb{N} excepté lui-même. Par exemple 6 est parfait : $6 = 1 + 2 + 3$.

Montrer que si $2^{n+1} - 1$ est un nombre premier alors $2^n(2^{n+1} - 1)$ est parfait.

Culturel : Ce résultat est déjà dans les éléments d'Euclide. La récip. est vraie : un nombre parfait pair est toujours de la forme précédente, c'est un résultat dû à Euler, qui ferait un autre exercice.

Solution 9 a) (i) L'idée de départ est l'identité remarquable $a^n - 1 = (a - 1)(a^{n-1} + \dots + a + 1)$ (†).

Si $a > 2$, alors $a - 1 > 1$ et $a^{n-1} + \dots + a + 1 > 1$, donc (†) donne une décomposition non triviale de a , et donc a n'est pas premier.

(ii) Si n n'est pas premier, alors comme $n \geq 2$, il admet une décomposition non triviale $n = pq$ où p et q sont deux entiers tels que $1 < p < n$ et $1 < q < n$.

Alors $a^{pq} - 1 = (a^p)^q - 1 = b^q - 1$ où $b = a^p$.

Et $b^q - 1 = (b - 1)(b^{q-1} + b^{q-2} + \dots + b + 1)$ (*).

Comme $b = a^p > 2$ car $a \geq 2$ et $p \geq 2$, on conclut que (*) donne une décomposition non triviale de $b^q - 1$ i.e. de $a^n - 1$. Donc $a^n - 1$ n'est pas premier.

b) Si $M = 2^{n+1} - 1$ est premier, alors $x = 2^n M$ est la D.F.P. de x , et donc l'ensemble $\Delta(x)$ des diviseurs de x dans \mathbb{N} est $\Delta(x) = \{2^k M^l, k \in \llbracket 0, n \rrbracket, l \in \llbracket 0, 1 \rrbracket\}$.

Donc la somme $\sigma(x)$ de tous les diviseurs premiers de x dans \mathbb{N} (avec x compris) s'écrit :

$$\sigma(x) = \sum_{k=0}^n 2^k + \sum_{k=0}^n 2^k M = \frac{1 - 2^{n+1}}{1 - 2} (M + 1) = (2^{n+1} - 1)2^{n+1} \quad \text{donc} \quad \sigma(x) = 2x \quad \text{et} \quad x \quad \text{est} \quad \text{parfait}. \quad \square$$

Exercice 10.

- a) Résoudre l'équation $x^2 + \overline{24}x + \overline{1} = \overline{0}$ dans $\mathbb{Z}/53\mathbb{Z}$.
b) Résoudre l'équation $\overline{x}^2 + \overline{6}.\overline{x} - \overline{13} = \overline{0}$ dans $\mathbb{Z}/21\mathbb{Z}$.

Solution 10

La grande différence entre les deux questions a) et b) : 53 est premier, alors que $21 = 3 \times 7$.
• Dans le a), on résout comme dans tous les corps (ou presque) : forme canonique ou formules avec Δ .
• Dans le b), on commence par décomposer $21 = 3 \times 7$ et on utilise le théorème Chinois (version facile) pour se ramener à deux équations modulo des nombres premiers comme au a). Ensuite recoller les morceaux encore avec le thme chinois.

a) **(M1) Avec la forme canonique :** dans $\mathbb{Z}/53\mathbb{Z}$:

$$x^2 + \overline{24}x + \overline{1} = (x + \overline{12})^2 - \overline{12}^2 + \overline{1} = (x + \overline{12})^2 - \overline{37}.$$

$$\text{Donc } (E) : x^2 + \overline{24}x + \overline{1} = \overline{0} \Leftrightarrow (x + \overline{12})^2 = \overline{37}.$$

On cherche une racine carrée de $\overline{37}$ dans $\mathbb{Z}/53\mathbb{Z}$. Par « force brute », on trouve que $\pm\overline{14}$ convient.

Donc $(E) \Leftrightarrow (x + \overline{12})^2 = (\overline{14})^2$ et par intégrité (savoir expliquer !), on en déduit que :

$$(E) \Leftrightarrow (x + \overline{12}) = \pm\overline{14} \Leftrightarrow x = \overline{2} \quad \text{ou} \quad x = -\overline{26}.$$

Donc les deux solutions de (E) dans $\mathbb{Z}/53\mathbb{Z}$ sont $\overline{2}$ et $-\overline{26}$.

(M2) Directement avec les formules connues (plutôt plus long !) *savoir expliquer qu'elles viennent simplement de la forme canonique.*

On considère $\Delta = \overline{24}^2 - 4 \times \overline{1} = \overline{42}$.

On cherche une racine carrée δ de $\overline{42}$ dans $\mathbb{Z}/53\mathbb{Z}$.

Par force brute du style :

```
for i in range(27):
    if (i**2)%53==42:
        print(i)
```

on trouve que $\delta = \overline{25}$ convient.

On sait alors que les deux solutions de (E) sont $\frac{-\overline{24} \pm \overline{25}}{2}$ et on trouve les mêmes solutions car $\overline{12} = -\overline{26}$ et $-\overline{49}/2 = \overline{4}/2 = \overline{2}$

Remarque 1 bien sûr la méthode « force brute » pour trouver les racines carrées diminue l'intérêt de cette question, on pourrait se dire qu'on teste tout aussi bien tous les $x \in \mathbb{Z}/53\mathbb{Z}$ dans l'équation mais bon ce serait quand même plus long : la recherche de racines carrées diminue le travail de plus que la moitié.

Remarque 2 (bonus !!) il existe bien sûr des méthodes plus rapides pour chercher une racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ pour p premier... c'est hélas beaucoup plus facile si $p \equiv -1 \pmod{4}$. Dans ce cas montrer que $(x)^{(p+1)/4}$ (qu'on peut calculer vite par exponentiation rapide) est bien une racine carrée de x .

b) Pour $x \in \mathbb{Z}$, on considère l'équation $(E) \ x^2 + 6x - 13 \equiv 0 \pmod{21}$.

Par théorème Chinois, comme $3 \wedge 7 = 1$, $(E) \Leftrightarrow \begin{cases} (E_1) & x^2 + 6x - 13 \equiv 0 \pmod{3} \\ \text{et} \\ (E_2) & x^2 + 6x - 13 \equiv 0 \pmod{7} \end{cases}$.

On résout (E_1) et (E_2) comme au a) car $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$ sont des corps. Précisément

$$(E_1) \Leftrightarrow \overline{x}^2 - \overline{1} = \overline{0} \text{ dans } \mathbb{Z}/3\mathbb{Z}.$$

$$\text{Donc } (E_1) \Leftrightarrow \overline{x} = \pm\overline{1} \text{ dans } \mathbb{Z}/3\mathbb{Z}.$$

$$\text{Donc } (E_1) \Leftrightarrow x \equiv \pm 1 \pmod{3}.$$

$$\text{De même } (E_2) \Leftrightarrow \overline{x}^2 - \overline{x} + \overline{1} = \overline{0} \text{ dans } \mathbb{Z}/7\mathbb{Z}.$$

$$\text{Par forme canonique } (E_2) \Leftrightarrow (\overline{x} - \frac{\overline{1}}{2})^2 - (\frac{\overline{1}}{2})^2 + \overline{1} = \overline{0}.$$

$$\text{Or dans } \mathbb{Z}/7\mathbb{Z}, \frac{\overline{1}}{2} = \overline{4} \text{ et } \overline{4}^2 = \overline{2} \text{ donc } (E_2) \Leftrightarrow (\overline{x} - \overline{4})^2 - \overline{1} = \overline{0} \Leftrightarrow (\overline{x} - \overline{4})^2 = \overline{1} \Leftrightarrow (\overline{x} - \overline{4}) = \pm\overline{1}.$$

Donc $(E_2) \Leftrightarrow \bar{x} = \bar{5}$ ou $\bar{x} = \bar{3} \Leftrightarrow x \equiv 3$ ou $x \equiv 5$ modulo 7.

$$\text{Retour à } (E) : (E) \Leftrightarrow \begin{cases} (E_1) \\ \text{et} \\ (E_2) \end{cases} \Leftrightarrow \begin{cases} (x \equiv 1 [3] \text{ ou } x \equiv -1 [3]) \\ \text{et} \\ (x \equiv 3 [7] \text{ ou } x \equiv 5 [7]) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 [3] \text{ et } x \equiv 3 [7] \\ \text{ou} \\ x \equiv 1 [3] \text{ et } x \equiv 5 [7] \\ \text{ou} \\ x \equiv -1 [3] \text{ et } x \equiv 3 [7] \\ \text{ou} \\ x \equiv -1 [3] \text{ et } x \equiv 5 [7] \end{cases}$$

Pour chacune des 4 lignes du dernier système de « ou », on a par théorème Chinois une unique solution modulo 21. Les déterminer !