Au Maroc, le programme de Mathématiques de la classe de Terminale ressemble à l'ancien programme de Mathématiques de la « Terminale C », filière d'excellence morte et enterrée depuis des années, et qui ne ressuscitera plus jamais. Les annales du bac marocain fourmillent de sujets magistraux, impensables dans la déliquescence des filières actuelles françaises, éminemment formateurs. Voici deux exercices d'arithmétique, posés à deux années d'intervalle, probablement rédigés par un même auteur (coup de chapeau à lui).

1

Un exercice culte du bac marocain 2023

Sujet

EXERCICE4 :(3 points)

Soit p **un nombre premier impair**. On considère dans $\mathbb{Z}$ l'équation (E) : $x^2 \equiv 2\ [p]$

0.25 1- a) Montrer que : $2^{p-1} \equiv 1\ [p]$

0.25 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1\ [p]$ ou $2^{\frac{p-1}{2}} \equiv -1\ [p]$

(On remarque que : $(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = 2^{p-1} - 1$)

2- Soit x une solution de l'équation (E)

0.5 a) Montrer que p et x sont premiers entre eux.

0.5 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1\ [p]$ (On pourra utiliser le théorème de Fermat)

0.25 3- Montrer que pour tout $k \in \{1,2,...,p-1\}$, p divise C_p^k

(On rappelle que : $(\forall k \in \{1,2,...,p-1\})$ $C_p^k = \dfrac{p!}{k!(p-k)!}$ et que : $kC_p^k = pC_{p-1}^{k-1}$)

0.25 4-a) En utilisant la formule de Moivre, montrer que :

$$(1+i)^p = 2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) + i2^{\frac{p}{2}} \sin\left(p\frac{\pi}{4}\right)$$

(i étant le nombre complexe tel que : $i^2 = -1$)

0.5 b) On admet que : $(1+i)^p = \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k} + i \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k+1}$

Montrer que : $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \in \mathbb{Z}$ et $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \equiv 1\ [p]$ (on pourra utiliser la question3-)

0.5 5- En déduire que si $p \equiv 5\ [8]$ alors l'équation (E) n'admet pas de solution dans $\mathbb{Z}$

Eléments de correction

Dans cet exercice, *p* est un nombre premier impair.

L'objectif est de résoudre dans $\mathbb{Z}$ l'équation $x^2 \equiv 2 \ (p)$.

.

2

1.a. Montrons d'abord que $2^p = 2 + (\text{multiple de } p)$

Considérons la formule du binôme lorsque l'exposant est égal à *p*. Pour tout réel *x* :

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} . x^k$$

En particulier, lorsque $x = 1$:

$$2^p = \sum_{k=0}^{p} \binom{p}{k} = \binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p-1} + \binom{p}{p}$$

Dans cette somme, le premier et le dernier terme sont égaux à 1 : $\binom{p}{0} = \binom{p}{p} = 1$.

Les autres, pour $1 \leq k \leq p-1$, sont des nombres entiers qui s'expriment ainsi : $\binom{p}{k} = \frac{p!}{k!.(p-k)!}$.

En tant que nombre premier, l'entier *p* est premier avec tous les entiers qui lui sont strictement inférieurs, donc premier avec leur produit. Il est premier avec les factorielles de *k* et de $p-k$, ainsi qu'avec le produit de ces factorielles. Le nombre entier $k!.(p-k)!$ divisant la factorielle de *p* et étant premier avec *p*, il divise la factorielle de $p-1$.

Pour tout entier *k* compris entre 1 et $p-1$, le coefficient $\binom{p}{k} = \frac{p!}{k!.(p-k)!}$ est donc un multiple de *p*. Leur somme est aussi un multiple de *p*.

Nous en déduisons que $2^p = 2 + (\text{multiple de } p)$ autrement dit que $2^p - 2$ est un multiple de *p*.

Démontrons maintenant que $2^{p-1} \equiv 1 \ (p)$.

Le nombre premier impair *p* divise $2^p - 2 = 2 \times (2^{p-1} - 1\ )$ et il est premier avec 2, d'après le théorème de Gauss, il divise $(2^{p-1} - 1\ )$.

Le nombre entier $2^{p-1} - 1$ est un multiple de *p*, autrement dit $2^{p-1} \equiv 1 \ (p)$.

3

1.b. L'entier *p* étant impair, son précédent $p - 1$ est un nombre pair et $\frac{p-1}{2}$ est un nombre entier. L'expression $2^{p-1} - 1$ apparaît comme étant une différence de deux carrés et est factorisable en : $2^{p-1} - 1 = \left(2^{\frac{p-1}{2}} - 1\right) \times \left(2^{\frac{p-1}{2}} + 1\right)$.

Nous savons que si un nombre premier divise un produit de facteurs, alors il divise au moins l'un des facteurs. Donc *p* divise l'un des deux facteurs au moins, ou bien $\left(2^{\frac{p-1}{2}} - 1\right)$ ou bien $\left(2^{\frac{p-1}{2}} + 1\right)$. Ainsi :

$$\begin{cases} 2^{\frac{p-1}{2}} - 1 \equiv 0 \ (p) \\ \text{ou bien} \\ 2^{\frac{p-1}{2}} + 1 \equiv 0 \ (p) \end{cases}$$

Le « ou bien » n'est *a priori* pas exclusif. Cependant, *p* ne peut pas diviser les deux facteurs à la fois, sinon il diviserait leur différence 2. Ce « ou bien » est en fait exclusif.

2. Soit *x* un entier solution de l'équation (E) : $x^2 \equiv 2 \ (p)$.

2.a. Montrons par contraposition que *x* et *p* sont premiers entre eux.

Soit *y* un nombre non premier avec *p*. Puisque *p* est un nombre premier, *y* est nécessairement un multiple de *p* et son carré est de ce fait lui aussi un multiple de *p*.

Si *y* n'est pas premier avec *p*, alors $y^2 \equiv 0 \ (p)$ et *y* **n'est pas** solution de l'équation (E).

Par contraposition, si *x* est un entier solution de l'équation (E), alors il est premier avec *p*.

2.b. D'après le petit théorème de Fermat, si *p* est un nombre premier et *a* un entier non divisible par *x*, alors $a^{p-1} \equiv 1 \ (p)$.

Appliquons le théorème de Fermat à la solution *x* de l'équation (E), dont on sait qu'elle n'est pas divisible par *p* : $x^{p-1} \equiv 1 \ (p)$. Or : $x^{p-1} = (x^2)^{\frac{p-1}{2}}$ et $x^2 \equiv 2 \ (p)$ donc $x^{p-1} \equiv 2^{\frac{p-1}{2}} \ (p)$.

4

Nous en déduisons : $2^{\frac{p-1}{2}} \equiv 1 \ (p)$

3. Résultat démontré dans le courant de notre méthode de résolution de la **question 1.a**.

4.a. Le nombre complexe $1 + i$ a pour module $\sqrt{2}$ et pour argument $\frac{\pi}{4}$ modulo 2π.

Sa forme trigonométrique est : $1 + i = \sqrt{2}.\left(\cos\left(\frac{\pi}{4}\right) + i.\sin\left(\frac{\pi}{4}\right)\right)$

Sa puissance *p*-ième a pour module $\left(\sqrt{2}\right)^p = 2^{\frac{p}{2}}$ et pour argument $p \times \frac{\pi}{4}$ modulo 2π.

Sa forme trigonométrique est : $(1+i)^p = 2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right) + i.\sin\left(p\frac{\pi}{4}\right)\right)$

Sa partie réelle est $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right)$ et sa partie imaginaire est $2^{\frac{p}{2}}.\left(\sin\left(p\frac{\pi}{4}\right)\right)$

4.b. La suite géométrique des puissances entières naturelles du nombre complexe *i* est une suite périodique de période 4.

Pour tout entier naturel *m* : $i^{4m} = 1$; $i^{4m+1} = i$; $i^{4m+2} = -1$; $i^{4m+3} = -i$.

Il est possible de condenser ces données en deux relations seulement :

Pour tout entier naturel *k* : $i^{2k} = (-1)^k$; $i^{2k+1} = (-1)^k \times i$.

Ce sont ces relations qui justifient la formule admise par l'énoncé. Pour tout entier naturel *n* :

$$(1+i)^n = \sum_{0 \le 2k \le n} (-1)^k.\binom{n}{2k} + i.\sum_{0 < 2k+1 \le n} (-1)^k.\binom{n}{2k+1}$$

Etudions plus précisément les premiers termes de la suite des puissances entières du nombre $1+i$.

Outre la relation $(1+i)^0 = 1$, nous obtenons les huit relations suivantes :

$(1+i)^1 = 1+i$	$(1+i)^2 = 2i$	$(1+i)^3 = -2+2i$	$(1+i)^4 = -4$
$(1+i)^5 = -4-4i$	$(1+i)^6 = -8i$	$(1+i)^7 = 8-8i$	$(1+i)^8 = 16 = 2^4$

5

De façon plus générale, soit *n* un entier naturel et $n = 8q + r$ avec $0 \leq r < 8$ sa division euclidienne par 8. Alors :

$$(1+i)^n = (1+i)^{8q+r} = (1+i)^{8q} \times (1+i)^r = 2^{4q} \times (1+i)^r$$

Ceci avec $(1+i)^r$ tel qu'il est donné dans le tableau précédent.

Le nombre $2^{\frac{n}{2}}.\left(\cos\left(n\frac{\pi}{4}\right)\right)$ est la partie réelle du nombre complexe obtenu. Du fait que les parties réelles des nombres $(1+i)^r$ du tableau sont toutes des entiers relatifs, le nombre $2^{\frac{n}{2}}.\left(\cos\left(n\frac{\pi}{4}\right)\right)$ est un entier relatif quelles que soient les circonstances.

En particulier, un nombre premier impair *p* peut être congru à 1, 3, 5 ou 7 modulo 8. Soit $p = 8q + r$ sa division euclidienne par 8. Détaillons les cas possibles qui se présentent pour $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right)$

- Si $p = 8q+1$, cas où $p \equiv 1\ (8)$, alors : $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = 2^{4q}$
- Si $p = 8q+3$, cas où $p \equiv 3\ (8)$, alors : $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = 2^{4q} \times (-2) = -2^{4q+1}$
- Si $p = 8q+5$, cas où $p \equiv 5\ (8)$, alors : $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = 2^{4q} \times (-4) = -2^{4q+2}$
- Si $p = 8q+7$, cas où $p \equiv 7\ (8)$, alors : $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = 2^{4q} \times 8 = 2^{4q+3}$

Dans tous les cas, $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right)$ est une puissance de 2.

De plus, en identifiant les parties réelles, nous disposons de la relation vue en début de question:

$$2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = \sum_{0 \leq 2k \leq p} (-1)^k.\binom{p}{2k}$$

Le nombre *p* étant impair, l'inégalité large $2k \leq p$ est en réalité une inégalité stricte, $2k < p$. La somme considérée contient le premier coefficient binomial $\binom{p}{0}$ mais ne contient pas le dernier $\binom{p}{p}$.

Par conséquent, en vertu de la **question 3**, les termes figurant dans la somme sont tous, sauf le premier qui est égal à 1, des multiples de *p*. Nous en déduisons que $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right)$ est égal à 1 plus un multiple de *p*, c'est-à-dire que, quel que soit le cas de figure :

6

$$2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) \equiv 1 \ (p).$$

5. Supposons que $p \equiv 5 \ (8)$. Alors, d'après la question précédente, $2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) = -2^{4q+2}$ où *q* est le quotient de la division euclidienne de *p* par 8, $p = 8q + 5$.

Nous obtenons dans ce cas la congruence : $-2^{4q+2} \equiv 1 \ (p)$

Or, dans ce cas, $4q + 2$ n'est autre que le nombre entier $\frac{p-1}{2}$, de sorte que nous obtenons la congruence : $2^{\frac{p-1}{2}} \equiv -1 \ (p)$.

Cette congruence exclut la congruence $2^{\frac{p-1}{2}} \equiv 1 \ (p)$ qui serait une conséquence de l'existence d'une solution à l'équation (E), s'il y en avait une.

Nous en déduisons que, si *p* est congru à 5 modulo 8, l'équation (E) ne peut pas avoir de solution.

Etudions les autres cas de figure.

- **Si $p = 8q + 1$, alors : $\frac{p-1}{2} = 4q$, donc $2^{\frac{p-1}{2}} = 2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) \equiv 1 \ (p)$**
- **Si $p = 8q + 3$, alors : $\frac{p-1}{2} = 4q + 1$, $2^{\frac{p-1}{2}} = -2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) \equiv -1 \ (p)$**
- **Si $p = 8q + 7$, alors : $\frac{p-1}{2} = 4q + 3$, $2^{\frac{p-1}{2}} = 2^{\frac{p}{2}}.\left(\cos\left(p\frac{\pi}{4}\right)\right) \equiv 1 \ (p)$**

En conclusion :

- **Si $p \equiv 3\ (8)$ ou si $p \equiv 5\ (8)$, la congruence $2^{\frac{p-1}{2}} \equiv -1\ (p)$ est vérifiée. Cette congruence est incompatible avec l'existence d'une solution de l'équation (E).**
- **Si $p \equiv 1\ (8)$ ou si $p \equiv 7\ (8)$, la congruence $2^{\frac{p-1}{2}} \equiv 1\ (p)$ est vérifiée. L'équation (E) peut avoir des solutions. Nous n'avons pas encore démontré que dans ce cas elle en avait effectivement. Cependant, remarquons que pour tout entier r tel que $1 \leq r \leq p-1$, $r^{p-1} \equiv 1\ (p)$, c'est-à-dire que $r^{\frac{p-1}{2}} \equiv \pm 1\ (p)$ et que ceux qui vérifient $r^{\frac{p-1}{2}} \equiv -1\ (p)$ ne sont pas congrus à un carré. Il en résulte que ceux qui vérifient $r^{\frac{p-1}{2}} \equiv 1\ (p)$ sont quant à eux congrus à un carré, ce qui est le cas en particulier de 2. Il y a effectivement des solutions.**

L'algorithme « bacmaroc » explore l'existence de solutions (modulo *p*) pour les nombres premiers situés entre 10 et 100.

```
>>> def bacmaroc():
        premiers=[11,13,17,19,23,29,31,37,41,43,47,53,61,67,71,73,79,83,97]
        for p in premiers:
                s=[]
                r=p%8
                for x in range(1,p):
                        if (x**2-2)%p==0:
                                s=s+[x]
                print(p,"est congru modulo 8 à",r,". Solutions :",s)
```

```
>>> bacmaroc()
11 est congru modulo 8 à 3 . Solutions : []
13 est congru modulo 8 à 5 . Solutions : []
17 est congru modulo 8 à 1 . Solutions : [6, 11]
19 est congru modulo 8 à 3 . Solutions : []
23 est congru modulo 8 à 7 . Solutions : [5, 18]
29 est congru modulo 8 à 5 . Solutions : []
31 est congru modulo 8 à 7 . Solutions : [8, 23]
37 est congru modulo 8 à 5 . Solutions : []
41 est congru modulo 8 à 1 . Solutions : [17, 24]
43 est congru modulo 8 à 3 . Solutions : []
47 est congru modulo 8 à 7 . Solutions : [7, 40]
53 est congru modulo 8 à 5 . Solutions : []
61 est congru modulo 8 à 5 . Solutions : []
67 est congru modulo 8 à 3 . Solutions : []
71 est congru modulo 8 à 7 . Solutions : [12, 59]
73 est congru modulo 8 à 1 . Solutions : [32, 41]
79 est congru modulo 8 à 7 . Solutions : [9, 70]
83 est congru modulo 8 à 3 . Solutions : []
97 est congru modulo 8 à 1 . Solutions : [14, 83]
>>>
```

Un exercice du bac marocain 2025

Sujet

8

EXERCICE3 : (3 points)

Soient p un nombre premier impair et a un entier premier avec p

0.5 1- Montrer que $a^{\frac{p-1}{2}} \equiv 1 \ [p]$ ou $a^{\frac{p-1}{2}} \equiv -1 \ [p]$

2- On considère dans $\mathbb{Z}$ l'équation : $ax^2 \equiv 1 \ [p]$. Soit x_0 une solution de cette équation.

0.5 a) Montrer que : ${x_0}^{p-1} \equiv 1 \ [p]$

0.25 b) En déduire que : $a^{\frac{p-1}{2}} \equiv 1 \ [p]$

3- Soit n un entier naturel non nul.

0.5 a) Montrer que si p divise $2^{2n+1}-1$ alors $2^{\frac{p-1}{2}} \equiv 1 \ [p]$

0.5 b) En déduire que l'équation (E) : $11x+\left(2^{2n+1}-1\right)y=1$ admet au moins une solution dans $\mathbb{Z}^2$

4- On considère dans $\mathbb{Z}$ l'équation (F) : $x^2+5x+2 \equiv 0 \ [11]$

0.25 a) Montrer que : $(F) \Leftrightarrow 2(2x+5)^2 \equiv 1 \ [11]$

0.5 b) En déduire que l'équation (F) n'admet pas de solution dans $\mathbb{Z}$

Eléments de correction

Dans cet exercice, *p* est un nombre premier impair.

9

1. Montrons d'abord par récurrence que pour tout entier strictement positif *a* : $a^p \equiv a\ (p)$

Initialisation. Cette propriété est vérifiée pour l'entier 1 : $1^p \equiv 1\ (p)$.

Hérédité. Supposons que pour un certain entier *a* strictement positif, la congruence $a^p \equiv a\ (p)$ soit vérifiée.

Considérons la formule du binôme lorsque l'exposant est égal à *p*. Pour tout réel *x* :

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} . x^k$$

En particulier, lorsque $x = a$:

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = \binom{p}{0} + \binom{p}{1} a + \cdots + \binom{p}{p-1} a^{p-1} + \binom{p}{p} a^p$$

Dans cette somme, pour $1 \leq k \leq p-1$, les coefficients binomiaux s'expriment ainsi : $\binom{p}{k} = \frac{p!}{k!.(p-k)!}$.

En tant que nombre premier, l'entier *p* est premier avec tous les entiers qui lui sont strictement inférieurs, donc premier avec leur produit. Il est premier avec les factorielles de *k* et de $p-k$, ainsi qu'avec le produit de ces factorielles. Le nombre entier $k!.(p-k)!$ divisant la factorielle de *p* et étant premier avec *p*, il divise la factorielle de $p-1$. Pour tout entier *k* compris entre 1 et $p-1$, le coefficient $\binom{p}{k} = \frac{p!}{k!.(p-k)!}$ est donc un multiple de *p*. Le nombre $\binom{p}{1} a + \cdots + \binom{p}{p-1} a^{p-1} + \binom{p}{p}$ est un multiple de *p*. Ainsi : $(a+1)^p = 1 + a^p + (\text{multiple de } p)$.

Nous en déduisons : $(a+1)^p \equiv 1 + a^p \quad (p)$ et compte tenu de l'hypothèse de récurrence :

$$(a+1)^p \equiv 1 + a \quad (p)$$

Il s'agit bien de la même congruence, écrite maintenant au rang $(a+1)$. La propriété à démontrer est héréditaire.

Conclusion : La propriété « $a^p \equiv a\ (p)$ » étant vérifiée pour $a = 1$ et étant héréditaire, elle est vérifiée pour tout entier *a* strictement positif.

Démontrons maintenant que si *a* est un un entier premier avec *p* : $a^{p-1} \equiv 1 \ (p)$.

Le nombre premier impair *p* divise $a^p - a = a \times (a^{p-1} - 1\ )$ et il est premier avec *a*, d'après le théorème de Gauss, il divise $(a^{p-1} - 1\ )$.

Le nombre entier $a^{p-1} - 1$ est un multiple de *p*, autrement dit $a^{p-1} \equiv 1 \ (p)$.

NB. Dans l'esprit de la classe de Terminale marocaine, le petit théorème de Fermat semble être au programme. Il suffisait donc de le citer et de partir de là sans reproduire la démonstration précédente.

L'entier *p* étant impair, son précédent $p - 1$ est un nombre pair et $\frac{p-1}{2}$ est un nombre entier. L'expression $a^{p-1} - 1$ apparaît comme étant une différence de deux carrés et est factorisable en : $a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \times \left(a^{\frac{p-1}{2}} + 1\right)$.

Nous savons que si un nombre premier divise un produit de facteurs, alors il divise au moins l'un des facteurs. Donc *p* divise l'un des deux facteurs au moins, ou bien $\left(a^{\frac{p-1}{2}} - 1\right)$ ou bien $\left(a^{\frac{p-1}{2}} + 1\right)$. Ainsi :

$$\begin{cases} a^{\frac{p-1}{2}} - 1 \equiv 0 \ (p) \\ \text{ou bien} \\ a^{\frac{p-1}{2}} + 1 \equiv 0 \ (p) \end{cases}$$

Le « ou bien » n'est *a priori* pas exclusif. Cependant, *p* ne peut pas diviser les deux facteurs à la fois, sinon il diviserait leur différence 2. Ce « ou bien » est en fait exclusif.

2. Soit x_0 un entier solution de l'équation (E) : $a \times x^2 \equiv 1 \ (p)$.

Cet entier vérifie la congruence : $a \times {x_0}^2 \equiv 1 \ (p)$.

2.a. Cette congruence implique, via le théorème de Bézout, que x_0 est un nombre premier avec *p*. En effet, elle signifie qu'il existe un entier relatif *k* tel que : $x_0.(ax_0) - k.p = 1$.

Nous pouvons appliquer le petit théorème de Fermat à l'entier x_0 : ${x_0}^{p-1} \equiv 1 \ (p)$.

2.b. En élevant à la puissance $(\frac{p-1}{2})$ les deux membres de la congruence vérifiée par x_0, nous obtenons une nouvelle congruence. Compte tenu que $(a \times {x_0}^2)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \times {x_0}^{p-1}$, nous obtenons la congruence :

$$a^{\frac{p-1}{2}} \times {x_0}^{p-1} \equiv 1 \ (p)$$

11

Compte tenu du résultat de **2.a**, cette congruence implique que :

$$a^{\frac{p-1}{2}} \equiv 1 \ (p).$$

3.a. Soit *n* un entier strictement positif. Supposons que *p* divise le nombre $2^{2n+1} - 1$.

Sous cette hypothèse, la congruence $2^{2n+1} \equiv 1 \ (p)$ est vérifiée, c'est-à-dire que $2 \times (2^n)^2 \equiv 1 \ (p)$

Le nombre $x_0 = 2^n$ est une solution de l'équation $2 \times x^2 \equiv 1 \ (p)$, type d'équation étudié dans la question précédente avec $a = 2$ (qui est premier avec *p* puisque *p* est un nombre impair).

D'après le résultat de cette question, nous obtenons :

S'il existe un entier *n* tel que *p* divise $2^{2n+1} - 1$, alors $2^{\frac{p-1}{2}} \equiv 1 \ (p)$.

3.b. **Considérons dans cette question le cas de $p = 11$. L'existence à démontrer dans cette question revient à prouver que les entiers 11 et $2^{2n+1} - 1$ sont des entiers premiers entre eux.**

Adaptons les conclusions de la **question 3.a** au présent contexte. Considérons le cas de $p = 11$.

Dans ce cas, $\frac{p-1}{2} = \frac{11-1}{2} = 5$. La puissance cinquième de 2 est le nombre : $2^5 = 32$, nombre qui est égal à $3 \times 11 - 1$ et qui vérifie la congruence : $2^5 \equiv -1 \ (11)$.

La congruence $2^5 \equiv 1 \ (11)$ n'est donc pas vérifiée. De ce fait, en contraposant la conclusion de la **question 2**, l'équation $2.x^2 \equiv 1 \ (11)$ n'admet pas de solution.

En contraposant pareillement la conclusion du **3.a** :

Puisque la congruence $2^5 \equiv 1\ (11)$ n'est pas vérifiée, quel que soit l'entier strictement positif *n*, le nombre premier 11 ne divise pas $2^{2n+1} - 1$. Et puisque 11 ne divise pas $2^{2n+1} - 1$, il est premier avec lui. De ce fait : il existe deux entiers relatifs *x* et *y* vérifiant la relation de Bézout, c'est-à-dire vérifiant :

12

$$11x + (2^{2n+1} - 1)y = 1$$

Quel que soit l'entier strictement positif *n*, l'équation $11x + (2^{2n+1} - 1)y = 1$ admet des solutions.

Des exemples de solutions pour quelques valeurs de l'entier *n* avec un algorithme Python

```
>>> def solutions(n):
        a=2**(2*n+1)
        s=[]
        for x in range(-a,a):
            for y in range(-11,11):
                if 11*x+a*y==1:
                    s=s+[[x,y]]
        print("exemples de solutions :",s)

>>> solutions(3)
exemples de solutions : [[-93, 8], [35, -3]]
>>> solutions(10)
exemples de solutions : [[-1143901, 6], [953251, -5]]
>>> solutions(1)
exemples de solutions : [[-5, 7], [3, -4]]
>>> solutions(2)
exemples de solutions : [[-29, 10], [3, -1]]
>>>
```

4.a. Tentons de démontrer l'équivalence $x^2 + 5x + 2 \equiv 0\ (11) \iff 2.(2x+5)^2 \equiv 1\ (11)$. Pour cela, commençons par développer l'expression $2.(2x+5)^2 - 1$ et à écrire à son sujet une congruence modulo 11. Nous obtenons $2.(2x+5)^2 - 1 = 8x^2 + 40x + 49 = 8x^2 + 40x + 5 + 4 \times 11$ donc :

$$2.(2x+5)^2 - 1 \equiv 8x^2 + 40x + 5\ (11)$$

Supposons que : $2.(2x+5)^2 - 1 \equiv 0\ (11)$ c'est-à-dire de façon équivalente supposons que :

$$8x^2 + 40x + 5 \equiv 0\ (11)$$

En remarquant que $8 \times 7 = 56 = 1 + 5 \times 11$, nous obtenons une nouvelle congruence en multipliant par 7 les deux membres de cette congruence :

$$2.(2x+5)^2 - 1 \equiv 0\ (11) \implies 7.(8x^2 + 40x + 5) \equiv 0\ (11)$$

Or, $7 \times 8 \equiv 1\ (11)$ et aussi $\begin{cases} 7 \times 40 = 280 = 27 \times 11 + 5 \\ 7 \times 5 = 35 = 3 \times 11 + 2 \end{cases}$ donc $\begin{cases} 7 \times 40 \equiv 5\ (11) \\ 7 \times 5 \equiv 2\ (11) \end{cases}$.

Compte tenu de la compatibilité de la relation de congruence avec les opérations dans $\mathbb{Z}$:

$$7.(8x^2 + 40x + 5) \equiv x^2 + 5x + 2\ (11)$$

13

Nous obtenons l'implication : $2.(2x+5)^2 - 1\ \equiv 0\ (11) \implies x^2 + 5x + 2 \equiv 0\ (11)$

Réciproquement, $x^2 + 5x + 2 \equiv 0\ (11) \implies 8x^2 + 40x + 16 \equiv 0\ (11)$ en multipliant par 8 les deux membres de la congruence et 16 étant congru à 5 modulo 11, nous avons l'implication réciproque

$$x^2 + 5x + 2 \equiv 0\ (11) \implies 8x^2 + 40x + 5 \equiv 0\ (11).$$

Il y a donc équivalence : $x^2 + 5x + 2 \equiv 0\ (11) \iff 2.(2x+5)^2 - 1\ \equiv 0\ (11).$

Or, nous avons montré précédemment que l'équation $2.X^2 - 1\ \equiv 0\ (11)$ n'avait pas de solution.

Il n'existe donc pas d'entier *x* tel que $2.(2x+5)^2 - 1\ \equiv 0\ (11)$.

L'équation (F) n'a pas non plus de solution.

Une recherche exhaustive avec un algorithme Python atteste que, quel que soit le reste de sa division par 11, le nombre $2.(2x+5)^2$ n'est jamais congru à 1 modulo 11, et le nombre $x^2 + 5x + 2$ n'est jamais congru à 0 modulo 11.

```
>>> def exhaustive():
        for x in range(0,11):
                y=2*((2*x+5)**2)
                z=x**2+5*x+2
                r=y%11
                s=z%11
                print("pour x=",x,"2(2x+5)^2 est congru à",r,"
et x^2+2x+5 est congru à",s)


>>> exhaustive()
pour x= 0 2(2x+5)^2 est congru à 6 et x^2+2x+5 est congru à 2
pour x= 1 2(2x+5)^2 est congru à 10 et x^2+2x+5 est congru à 8
pour x= 2 2(2x+5)^2 est congru à 8 et x^2+2x+5 est congru à 5
pour x= 3 2(2x+5)^2 est congru à 0 et x^2+2x+5 est congru à 4
pour x= 4 2(2x+5)^2 est congru à 8 et x^2+2x+5 est congru à 5
pour x= 5 2(2x+5)^2 est congru à 10 et x^2+2x+5 est congru à 8
pour x= 6 2(2x+5)^2 est congru à 6 et x^2+2x+5 est congru à 2
pour x= 7 2(2x+5)^2 est congru à 7 et x^2+2x+5 est congru à 9
pour x= 8 2(2x+5)^2 est congru à 2 et x^2+2x+5 est congru à 7
pour x= 9 2(2x+5)^2 est congru à 2 et x^2+2x+5 est congru à 7
pour x= 10 2(2x+5)^2 est congru à 7 et x^2+2x+5 est congru à 9
>>>
```