Exercice 0 On va décomposer $10!$ en produit de facteurs premiers.

$10! = 2\times3\times4\times5\times6\times7\times8\times9\times10$

$10! = 2\times3\times2^2\times5\times2\times3\times7\times2^3\times3^2\times2\times5 = 2^8\times3^4\times5^2\times7^1$

D'après le cours, le nombre N de diviseurs de $10!$ est égal à : $N = (8+1)\times(4+1)\times(2+1)\times(1+1) = 9\times5\times3\times2 = \boxed{270}$

Exercice 1 $x, y, z \in \mathbb{N}^*$ et $x^2+y^2=z^2$. $(x;y;z)$ est appelé un T.P.

Partie A Soit $(x;y;z)$ un T.P et $p\in\mathbb{N}^*$.

1) On a : $(px)^2+(py)^2 = p^2x^2+p^2y^2 = p^2(x^2+y^2) \overset{\text{car } x^2+y^2=z^2 \text{ vu que } (x;y;z) \text{ est un T.P!}}{=} p^2z^2 = (pz)^2$

Par suite, $(px;py;pz)$ est un T.P.

2) Supposons que $x^2+y^2=z^2$. Montrons que x, y et z non tous impairs.

On raisonne par l'absurde : sous l'hypothèse où x, y et z seraient tous les trois impairs on aurait :

$x\equiv1(2)$; $y\equiv1(2)$ et $z\equiv1(2)$, donc $x^2\equiv1(2)$; $y^2\equiv1(2)$ et $z^2\equiv1(2)$. (compatibilité de $\equiv$ avec les puissances)

Par suite, $x^2+y^2\equiv1+1\,(2)\equiv0\,(2)$ et $z^2\equiv1(2)$, donc $x^2+y^2\not\equiv z^2\,(2)$: Ceci est absurde, car par donnée, $x^2+y^2=z^2$, donc $x^2+y^2\equiv z^2(2)$. $[a=b \Rightarrow \forall m\in\mathbb{N}^*, a\equiv b(m)]$.

Ainsi $x;y;z$ ne sont pas tous les trois impairs.

3) $n\in\mathbb{N}^*$. $\exists\alpha\in\mathbb{N}$ et $\exists k\in\mathbb{N}$ avec k impair tel que : $n=2^\alpha\cdot k$.

a) $192 = 2\times96 = 2\times2\times48 = 2\times2\times2\times24 = 2\times2\times2\times2\times12 = 2\times2\times2\times2\times2\times2\times3 = 2^6\times3$

La décomposition de 192 est donc $2^6\times3$.

b) $x=2^\alpha\times k$ et $z=2^\beta\times m$ avec k et m impairs.

Donc $x^2=(2^\alpha\times k)^2=(2^\alpha)^2\times k^2=2^{2\alpha}\times k^2$ et $2x^2=2^1\times x^2=2^1\times2^{2\alpha}\times k^2=2^{2\alpha+1}\times k^2$

Vu que k est impair, il en est de même pour k^2, de sorte que la décomposition de $2x^2$ est : $2^{2\alpha+1}\times k^2$.

De même, $z^2=(2^\beta\times m)^2=(2^\beta)^2\times m^2=2^{2\beta}\times m^2$ avec m^2 impair car m impair, donc sa décomposition de z^2 est $2^{2\beta}\times m^2$.

c) Supposons (on raisonne par l'absurde) qu'il existe un couple d'entiers non nuls $(x;z)$ tel que : $2x^2=z^2$.

Alors grâce à b), l'exposant de 2 dans la décomposition de $2x^2$ vaut $2\alpha+1$, avec $\alpha\in\mathbb{N}$, donc $2\alpha+1$ est impair.

l'exposant de 2 dans la décomposition de z^2 vaut 2β, avec $\beta\in\mathbb{N}$, donc 2β pair.

Si $2x^2=z^2$, alors les entiers $2x^2$ et z^2 ont la même décomposition, donc en particulier la même puissance de 2 : (unicité de la décomposition!).

par suite, $2\alpha+1=2\beta$: absurde (IMPAIR = PAIR !!).

Donc il n'existe aucun couple d'entiers non nuls $(x;z)$ tel que $2x^2=z^2$.

Pour la suite, pour tout T.P $(x;y;z)$ on range x, y, z par ordre croissant : $x<y<z$ (impossible d'avoir $x=y$ grâce à 3c) ....

Partie B

1)
$$\begin{array}{r|l} 2015 & 5 \\ 403 & 13 \\ 31 & 31 \\ 1 & \end{array}$$
On a : $\boxed{2015 = 5 \times 13 \times 31}$.

$(3;4;5)$ est un T.P. et $2015 = 5 \times (13 \times 31) = 5 \times 403$

Grâce à A_2 appliqué avec $p = 403$, on déduit que : $(3 \times 403 ; 4 \times 403 ; 5 \times 403)$ est un T.P, à savoir que :

$(1209 ; 1612 ; 2015)$ est un T.P.

2) Un peu d'intuition ! $2n+1 = 2015$, donc $n = 1007$.

Vu que $(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2$, $(2n+1 ; 2n^2+2n ; 2n^2+2n+1)$ est un T.P.

On veut que : $(2015 ; y ; z) = (2n+1 ; 2n^2+2n ; 2n^2+2n+1)$, donc on pose : $\begin{cases} y = 2n^2+2n = 2n(n+1) \\ z = 2n^2+2n+1 \end{cases}$

$y = 2 \times 1007 \times 1008 = 2.030.112$ et $z = 2 \times 1007^2 + 2 \times 1007 + 1$

$z = 2.030.113$

$(2015 ; 2.030.112 ; 2.030.113)$ est un T.P.

3a) $403^2 = 169 \times 961$. $\begin{cases} z^2 - x^2 = 403^2 \\ x, z \text{ non nuls} \end{cases}$

$403^2 = 13^2 \times 31^2$

Or $z^2 - x^2 = (z-x)(z+x)$ avec $0 < x < 403$ et $x < z$.

Donc : $(z-x)(z+x) = 13^2 \times 31^2$. et $z - x < z + x$.

Par exemple : $\begin{cases} z - x = 13^2 \\ z + x = 31^2 \end{cases} \iff \begin{cases} z - x = 169 \\ 2z = 13^2 + 31^2 \end{cases} \iff \begin{cases} x = z - 169 \\ z = \frac{1130}{2} = 565 \end{cases} \iff \begin{cases} x = 396 \\ z = 565 \end{cases}$

Le couple : $(396 ; 565)$ est solution de : $z^2 - x^2 = 403^2$ avec $x < 403$.

3b) On a grâce à 3a) : $565^2 - 396^2 = 403^2$, donc : $396^2 + 403^2 = 565^2$: $(396 ; 403 ; 565)$ est donc un T.P.

Or, $2015 = 5 \times 403$, donc grâce à A_2 appliqué avec $p = 5$, on déduit que : $(5 \times 396 ; 5 \times 403 ; 5 \times 565)$ est un autre T.P.

Soit $(x ; 2015 ; z) = (1980 ; 2015 ; 2825)$ est un T.P.

Exercice II

1)

m	2	2	2	3	3	3	4	4	4
n	2	3	4	2	3	4	2	3	4
ord. à l'origine de (MN)	4	6	8	6	9	12	8	12	16

3) Les ordonnées de ces points là (non traversés par l'un des sujets) sont des nombres premiers. (Vu qu'ils ne s'écrivent pas comme produits de 2 facteurs strictement supérieurs à 1) !

2) $M(m ; m^2)$ et $N(-n ; (-n)^2)$ donc $N(-n ; n^2)$. $M \neq N$ car $x_N \neq x_M$ vu que $x_M > 0$ et $x_N < 0$.

$\boxed{a}$ = coeff. directeur de $(MN) = \frac{y_M - y_N}{x_M - x_N} = \frac{m^2 - n^2}{m - (-n)} = \frac{m^2 - n^2}{m+n} = \frac{(m-n)(m+n)}{(m+n)} = \boxed{m - n}$.

(MN) a pour équation réduite : $y = (m-n)x + p$. Or $M(m ; m^2) \in (MN)$ ssi $m^2 = (m-n) \times m + p$

ssi $m^2 = m^2 - mn + p$

ssi $p = mn$.

(MN) a donc pour équation réduite : $y = (m-n)x + mn$. Son ordonnée à l'origine est égale mn.

Exercice 4 : Le petit théorème de Fermat.

Partie 1 $a \in \mathbb{N}^*$; $n \in \mathbb{N}^*$.

(1a) Facile.

(1b) Pour $n \in \{2 ; 3 ; 5 ; 7\}$.

(2a) On suppose que $\forall a \in \mathbb{N}^*$, $n \mid a^n - a$.

Or, $a^n - a = a(a^{n-1} - 1)$, donc $n \mid a(a^{n-1} - 1)$. Si de plus $PGCD(a ; n) = 1$, alors d'après le théorème de Gauss, $n \mid a^{n-1} - 1$ ∎

(2b) Si $n \in \mathbb{P}$, alors $\forall a \in \mathbb{N}^*$, on a (cf. cours) : $n \mid a$ ou bien $PGCD(n ; a) = 1$.

Si a n'est pas un multiple de n, alors $n \nmid a$, donc comme $n \in \mathbb{P}$, on a : $PGCD(n ; a) = 1$.

Comme $n \mid a(a^{n-1} - 1)$ et que $PGCD(n ; a) = 1$, grâce à la question (2a), on déduit que $n \mid a^{n-1} - 1$ ∎

(2c) On suppose que $n \mid a$: Donc $a \equiv 0 \, (n)$.

Par suite, si $n - 1 \in \mathbb{N}^*$, on a : $a^{n-1} \equiv 0^{n-1} \, (n)$, c'est à dire : $a^{n-1} \equiv 0 \, (n)$.

Par suite, $a^{n-1} - 1 \equiv 0 - 1 \, (n)$, donc : $a^{n-1} - 1 \equiv -1 \, (n)$.

Donc $n \nmid (a^{n-1} - 1)$, car sinon, on aurait eu $a^{n-1} - 1 \equiv 0 \, (n)$ ce qui n'est pas le cas. ($-1 \not\equiv 0 \, (n)$) pour $n \geq 2$.

Remarque : il y a ici une inexactitude dans l'énoncé : le résultat demandé n'est valable que si $n \geq 2$.

(2d) Illustration : Pour 2a) : Pour $n = 2$, $\forall a \in \mathbb{N}^*$, $a^2 - a$ est divisible par 2 vu que $a^2 - a = a(a-1)$

et que si $a \equiv 0 \, (2)$, alors $a(a-1) \equiv 0 \, (2)$ et si $a \equiv 1 \, (2)$, alors $a - 1 \equiv 0 \, (2)$, donc $a(a-1) \equiv 0 \, (2)$.

Prenons $a = 15$ $PGCD(n ; a) = PGCD(2 ; 15) = 1$, donc toutes les hypothèses nécessaires pour appliquer 2a) sont satisfaites, donc $2 \mid 15^{2-1} - 1$ i.e $2 \mid 14$ (ouf !).

Pour le 2b) : Prenons l'exemple précédent !! $n = 2$ et $a = 15$ toujours : 15 n'est pas un multiple de 2 et $PGCD(2 ; 15) = 1$, donc $15^{2-1} - 1 = 14$ est divisible par $n = 2$.

Pour le 2c) : Prenons $n = 2$ et $a = 4$: $a = 2n$, donc a est un multiple de n.

et $4^{2-1} - 1 = 3$ et 3 n'est pas divisible par 2.

Partie 2 $A = \{a ; 2a ; \dots ; (p-1)a\} = \{ka ; k \in [\![1 ; p-1]\!]\}$. et $\begin{cases} p \in \mathbb{P} \\ a \in \mathbb{N} \text{ et } p \nmid a. \end{cases}$

① Vu que $p \in \mathbb{P}$, p est premier avec tout entier qu'il ne divise pas. donc

$\forall k \in [\![1 ; p-1]\!]$, $PGCD(p ; k) = 1$ (les entiers $< \grave{a}\ p$ ne sont pas divisibles par p).

Supposons par l'absurde qu'il existe $k \in [\![1 ; p-1]\!]$ tel que : $p \mid ka$. Vu que $PGCD(p ; k) = 1$, d'après le Th. de Gauss, on aurait $p \mid a$: Ceci est absurde, car par donnée, $p \nmid a$.

Conclusion : $\boxed{p \text{ ne divise aucun des éléments de } A}$

② a) $\exists! (\alpha ; \beta) \in \mathbb{N} \times \mathbb{N}$ tel que : $ka = p\alpha + \beta$ avec : $0 \leq \beta < p$ d'après le Th. de la D.E.

Si $\beta = 0$, alors $ka = p\alpha$, donc $p \mid ka$ en contradiction avec le résultat de la question précédente. donc $\beta \neq 0$.

b) Soit k et l deux entiers de $[\![1 ; p-1]\!]$ tels que $k \times a$ et $l \times a$ ont le même reste dans la D.E par p.

On a donc : $k \times a \equiv l \times a \ (p)$, donc $p \mid ka - la$, donc $p \mid a(k-l)$.

Or $p \nmid a$ par donnée et $p \in \mathbb{P}$, donc $PGCD(p ; a) = 1$ et $p \mid a(k-l)$, donc d'après le Th. de Gauss $p \mid k - l$. De plus $1 \leq k \leq p-1$
$1 \leq l \leq p-1$, donc $1-p \leq -l \leq -1$ et $0 \leq k - l \leq p-2 < p$. Le seul multiple de p situé dans $[0, p-2]$ est 0. Donc $k - l = 0$, donc $k = l$, donc $ka = la$ ∎

c) Vu que les éléments de A sont 2 à 2 distincts, en contraposant le résultat de la question précédente, on obtient : les éléments de A ont des restes 2 à 2 distincts.

Or A est composé de $p-1$ éléments et chacun des restes est un entier compris entre 0 (exclu ! cf. 2a) et $p-1$ inclus donc entre 1 et $p-1$.

Par suite, sans tenir compte de l'ordre des restes, la liste de ces restes est exactement l'ensemble $\{1 ; 2 ; \dots ; p-1\}$.

③ $P = a \times 2a \times \dots \times (p-1)a$

ⓐ Grâce à la question précédente, la liste non ordonnée des restes de $a ; 2a ; \dots ; (p-1)a$ dans la D.E par p est $\{1 ; 2 ; \dots ; p-1\}$. donc chacun des éléments de A est congru, modulo p, à l'un des éléments de $\{1 ; 2 ; \dots p-1\}$. Par compatibilité de la relation de congruence avec le produit, P (le produit des éléments de A) est donc congru au produit des éléments $1 \times 2 ; \dots ; p-1$ modulo p.

Donc $P \equiv 1 \times 2 \times \dots \times (p-1) \ (p)$.

ⓑ $P = a \times 2a \times \dots \times (p-1)a = 1 \times 2 \times \dots \times (p-1) \times \underbrace{a \times a \times \dots \times a}_{p-1 \text{ facteurs}} = 1 \times 2 \times \dots \times (p-1) \times a^{p-1}$.

3c) On a : $p = 1\times 2\times \cdots \times (p-1)\times a^{p-1}$, donc $p \equiv 1\times 2\times \cdots \times (p-1)\times a^{p-1}\ (p)$ et aussi, grâce à 3a), $p \equiv 1\times 2\times \cdots \times (p-1)\ (p)$.

Par transitivité de la relation de congruence, on a : $1\times 2\times \cdots \times (p-1)\times a^{p-1} \equiv 1\times 2\times \cdots \times (p-1)\ (p)$.

Donc : $1\times 2\times \cdots \times (p-1)\times a^{p-1} - 1\times 2\times \cdots \times (p-1) \equiv 0\ (p)$

Donc : $[1\times 2\times \cdots \times (p-1)]\times (a^{p-1}-1) \equiv 0\ (p)$.

3d) Grâce à 3c), on a : $p \mid [1\times 2\times \cdots \times (p-1)]\times (a^{p-1}-1)$.

De plus p est premier avec tout nombre qu'il ne divise pas car $p \in \mathbb{P}$, donc p est premier avec chacun des entiers $1, 2, \ldots, p-1$, donc (# le cours !), p est premier avec $1\times 2\times \cdots \times (p-1)$.

Ainsi on a : $\begin{cases} p \mid [1\times \cdots \times (p-1)]\times (a^{p-1}-1) \\ PGCD(p\,;\,1\times 2\times \cdots \times (p-1)) = 1 \end{cases}$, donc d'après le th. de Gauss, $p \mid a^{p-1}-1$

(4) On sait à présent que si $p \in \mathbb{P}$ et si $a \in \mathbb{N}$ tel que $p \nmid a$, alors $p \mid a^{p-1}-1$ (Petit th. de Fermat).
Montrons que $\forall a \in \mathbb{N}^*$, $p \mid a^p - a$:

Soit $a \in \mathbb{N}^*$: *) Si $p \nmid a$, alors grâce au Petit Fermat, $p \mid a^{p-1}-1$, donc p divise tout multiple de $a^{p-1}-1$, en particulier, $p \mid a(a^{p-1}-1)$ donc $p \mid a^p - a$.

**) Si $p \mid a$: alors p divise tout multiple de a, en particulier, vu que $a^{p-1}-1 \in \mathbb{N}$ ($p \geq 2$, donc $p-1 \geq 1$ donc $a^{p-1} \geq 1$)
$p \mid a(a^{p-1}-1)$, bref $p \mid a^p - a$.

Dans les deux cas, on a bien : $\boxed{\forall a \in \mathbb{N}^*,\ p \mid a^p - a}$

Partie 3

(1a) $2^{10}-1 = 2^{11-1}-1$ avec $11 \in \mathbb{P}$. $11 \nmid 2$, donc d'après le Petit Fermat, $11 \mid 2^{11-1}-1$
Donc $11 \mid 2^{10}-1$.

(1b) $4^{16}-4$
(1c) $4^{14}-4$ sont clairement divisibles par 2 avec $2 \in \mathbb{P}$! $\begin{pmatrix} 4^{16}-4 = 2^{32}-4 = 2(2^{31}-2) \\ 4^{14}-4 = 2(2^{27}-2) \end{pmatrix}$.

(2) $6^6-1 = 6^{7-1}-1$ avec $7 \in \mathbb{P}$. Vu que $7 \nmid 6$, on a d'après le Petit Fermat : $7 \mid 6^{7-1}-1$ i.e $7 \mid 6^6-1$. On a donc : $6^6-1 \equiv 0\ (7)$, donc $6^6 \equiv 1\ (7)$, par suite $6^6+6 \equiv 1+6\ (7)$
donc $6^6+6 \equiv 0\ (7)$, donc $7 \mid 6^6+6$.

De plus, $6 \mid 6^6+6$ vu que $6^6+6 = 6(\underbrace{6^5+1}_{\in \mathbb{N}})$.

Ainsi : $\begin{cases} 7 \mid 6^6+6 \\ 6 \mid 6^6+6 \end{cases}$. Vu que $PGCD(6\,;7) = 1$, d'après un corollaire du th. de Gauss, $7\times 6 \mid 6^6+6$ i.e $42 \mid 6^6+6$.

③ $999999 = 10^6 - 1 = 10^{7-1} - 1$ avec $7 \in \mathbb{P}$. De plus, $7 \nmid 10$, donc toujours d'après le petit Fermat, on a : $7 \mid 10^{7-1} - 1$ i.e $7 \mid 10^6 - 1$, donc 7 est un diviseur premier de 999 999.

④ $n \in \mathbb{N}$ et $a = n^5 - n$.

ⓐ On raisonne modulo 2 : *) Si $n \equiv 0(2)$, alors $n^5 \equiv 0(2)$, donc $n^5 - n \equiv 0 - 0\,(\,)$, donc $n^5 - n \equiv 0(2)$

Donc $a \equiv 0(2)$, donc $2 \mid a$.

**) Si $n \equiv 1(2)$, alors, $n^5 \equiv 1^5(2)$, donc $n^5 \equiv 1(2)$, donc $n^5 - n \equiv 1-1\,(2)$, donc $n^5 - n \equiv 0(2)$

Donc $a \equiv 0(2)$, donc $2 \mid a$.

Ainsi, $\underline{\forall n \in \mathbb{N}, 2 \mid n^5 - n}$.

Raisonnement analogue modulo 3 avec un cas de plus à distinguer.... ($n \equiv 0(3)$ ou $n \equiv 1(3)$ ou $n \equiv 2(3)$)

$\Downarrow$ $n^5 \equiv 0(3)$ Donc $n^5 - n \equiv 0(3)$ | $n^5 \equiv 1(3)$ Donc $n^5 - n \equiv 0(3)$ | $n^5 \equiv 2^5(3)$ $n^5 - n \equiv 30(3)$ $\equiv 0(3)$.

ⓑ Vu que $5 \in \mathbb{P}$, on applique le corollaire du petit Fermat :

∴ $\forall n \in \mathbb{N}$, $n^5 - n$ est divisible par 5, donc $\underline{a \text{ est divisible par } 5}$.

ⓒ Grâce à 4a) et 4b) : $\begin{cases} 2 \mid a \\ 3 \mid a \\ 5 \mid a \end{cases}$, de plus $PGCD(2;3) = 1$, donc (# corollaire du th. de Gauss), $6 \mid a$.

Ainsi : $\begin{cases} 6 \mid a \\ 5 \mid a \end{cases}$ et $PGCD(6;5) = 1$, donc de même, $6 \times 5 \mid a$ i.e $\boxed{30 \mid a}$.

⑤ $\forall n \in \mathbb{N}$, $a = n^{13} - n$.

ⓐ Idem qu'en (4a) !

ⓑ $a = n^{13} - n$

Vu que $13 \in \mathbb{P}$, grâce au corollaire du petit Fermat, $13 \mid n^{13} - n$, donc $\underline{13 \mid a}$.

$a = n^{13} - n = n(n^{12} - 1) = n((n^6)^2 - 1^2) = n(n^6 - 1)(n^6 + 1)$. (*)

Or, $n^6 - 1 = n^{7-1} - 1$, donc si $7 \nmid n$, alors grâce au petit Fermat, $7 \mid n^6 - 1$, et par suite, $7 \mid a$ car grâce à (*), a est un multiple de $n^6 - 1$.

Si $7 \mid n$, alors comme a est un multiple de n (grâce à (*)), $7 \mid a$.

Donc $\boxed{\text{a est divisible par 13 et par 7}}$

ⓒ On a : $\begin{matrix} 2 \mid a \\ 3 \mid a \\ 13 \mid a \\ 7 \mid a \end{matrix}$ et 2, 3, 13 et 7 sont des nombres premiers 2 à 2 distincts, donc $2 \times 3 \times 13 \times 7 \mid a$ à savoir :

$\boxed{546 \mid a.}$

⑥ $p \in \mathbb{P}$ et $p \mid 2^p + 5$.

ⓐ Grâce au corollaire du petit Fermat, vu que $2 \in \mathbb{P}$, $\forall p \in \mathbb{P}$, $2 \mid 2^p - 2$.

b) $\begin{cases} p \mid 2^p+5 \\ p \mid 2^p-2 \end{cases} \Longrightarrow p \mid 2^p+5-(2^p-2)$ donc $p \mid 7$. Vu que $p \in \mathbb{P}$, on déduit que $\boxed{p=7}$.

7 est l'unique valeur de p telle que p divise 2^p+5.

7) $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$.

a) $p \in \mathbb{P}$, donc $\forall a \in \mathbb{Z}$, $p \mid a^p - a$ (corollaire du Petit Fermat).
$\forall b \in \mathbb{Z}$, $p \mid b^p - b$

Si de plus $p \mid a+b$, alors p divise la somme suivante : $\underbrace{a^p-a}_{\text{multiple de } p} + \underbrace{b^p-b}_{\text{multiple de } p} + \underbrace{a+b}_{\text{multiple de } p} = a^p+b^p$.

Donc $\boxed{\text{si } p \in \mathbb{P} \text{ et si } p \mid a+b, \text{ alors, } p \mid a^p+b^p}$

b) $11 \mid 5+6$, donc par application directe de 7a), $11 \mid 5^{11}+6^{11}$ (ici $p=11$).
Avec une calculatrice, on vérifie sans peine que $11 \mid 5^{11}+6^{11}$ vu que $5^{11}+6^{11} = 411625181$ et que le critère de divisibilité par 11 est ici utilisable car : $4+1+2+1+1-(1+6+5+8) = -11$ et $-11 \equiv 0\ (11)$.

c) On cherche $p \in \mathbb{P}$ tel que $p \mid 5+7 = 12$. $p \in \{2;3\}$.
$5^2+7^2 = 74$ et $2 \mid 74$ ($5^3+7^3 = 468$ et $3 \mid 468$). $\begin{cases} p \mid 5+7 \\ p \in \mathbb{P} \end{cases}$ grâce à 7a), $p \mid 5^p+7^p$.

d) De même en a) : si $p \in \mathbb{P}$, si $p \mid a-b$, alors $p \mid a^p-b^p$ (mais seulement dans $\mathbb{Z}$ ici).
On prend $p=7$: $7 \mid 11-4$, donc # a), vu que $7 \in \mathbb{P}$, $7 \mid 11^p-4^p$ ∎