16 Montrer que pour tout $n \in \mathbb{N}$

1. $6 \mid 5n^3+n$
2. $7 \mid 3^{2n+1}+2^{n+2}$
3. $5 \mid 2^{2n+1}+3^{2n+1}$
4. $11 \mid 3^{8n}5^4+5^{6n}7^3$
5. $9 \mid 4^n-1-3n$
6. $15^2 \mid 16^n-1-15n$.

1 – $5n^3+n \equiv 0\ [6]$?

1ère méthode : tester tous les entiers modulo 6.

ex : $n \equiv 4 [6]$ ie $n \equiv -2 [6]$

$5n^3+n \equiv -5\times 2^3 - 2\ [6]$
$\equiv 1\times 2 - 2\ [6]$
$\equiv 0\ [6]$

2e méthode :

$5n^3+n \equiv n(5n^2+1)\ [6]$
$\equiv -n(n^2-1)\ [6]$
$\equiv \underbrace{-n(n-1)(n+1)}_{\text{3 entiers consécutifs}}\ [6]$

donc divisible par 2 et 3 et $2\wedge 3 = 1$, donc par 6.

$\equiv 0\ [6]$

4 – But : $11 \mid 3^{8n}5^4+5^{6n}7^3$

$3^2 = 9 \equiv -2\ [11]$

$3^{8n} = (3^2)^{4n} \equiv 2^{4n}\ [11]$
$\equiv 4^{2n}\ [11]$
$\equiv 5^n\ [11]$

$5^2 \equiv 3\ [11]$ donc $5^{6n} = (5^2)^{3n} \equiv 3^{3n}\ [11]$

$3^3 = 9\times 3 \equiv -2\times 3\ [11]$
$\equiv -6\ [11]$
$\equiv 5\ [11]$

donc $5^{6n} \equiv 5^n\ [11]$.

$5^4 \equiv 3^2\ [11]$
$\equiv -2\ [11]$

$7^3 \equiv (-4)^3\ [11]$
$\equiv -16\times 4\ [11]$
$\equiv -5\times 4\ [11]$
$\equiv -9\ [11]$
$\equiv 2\ [11]$

Finalement, $3^{8n}5^4+5^{6n}7^3 \equiv -2\times 5^n + 2\times 5^n\ [11]$
$\equiv 0\ [11]$.

6 But : $15^2 \mid 16^n-1-15n$

$16^n-1-15n = (16-1)\times \sum_{k=0}^{n-1} 16^k - 15n = 15\times \underbrace{\left(\sum_{k=0}^{n-1}16^k - n\right)}_{\text{divisible par 15?}}$

Or $\sum_{k=0}^{n-1} 16^k - n \equiv \sum_{k=0}^{n-1} 1 - n\ [15]$
$\equiv 0\ [15]$

Autre méthode : $16^n-1-15n = (15+1)^n - 1 - 15n = \sum_{k=2}^{n} \binom{n}{k} 15^k$
$= 15^2 \times \sum_{k=2}^{n} \binom{n}{k} 15^{k-2}$

17 Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

$(S)\begin{cases} N \equiv 3\ [17] \\ N \equiv 4\ [11] \\ N \equiv 5\ [6] \end{cases}$ 17, 11, 6 premiers entre eux 2 à 2.

1ère méthode :

$(S) \Leftrightarrow \exists k, \ell, n \in \mathbb{Z},\ N = \boxed{3+17k = 4+11\ell} = 5+6n$

et résoudre les équa° diophantienne

2e méthode : $(S) \Leftrightarrow \begin{cases} N \equiv 37\ [\underbrace{11\times17}_{187}] \\ N \equiv 5\ (6) \end{cases}$

$17 \wedge 11 = 1$, thm chinois

$2\times17 + (-3)\times11 = 1$ donc solu part de $\begin{cases} N \equiv 3\ (17) \\ N \equiv 4\ (11) \end{cases}$ $c = 4\times2\times17 - 3\times3\times11 = 37$

$187 \wedge 6 = 1$: thm chinois $(S) \Leftrightarrow N = -5947\ [\underbrace{11\times17\times6}_{=1122}]$

Euclide : $187 = 6\times31 + 1$ ie $187 - 6\times31 = 1$

solu° particulière : $5\times187 - 37\times6\times31 = -5947$

donc $(S) \Leftrightarrow N \equiv \boxed{785}\ [1122]$

Généralisa° (HP) du thm chinois : $(S) \Leftrightarrow N \equiv c\ [11\times17\times6]$

car 11, 17, 6 2 à 2 1er entre eux

où c solu° particulière.

$(a)+(b) = a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

$ax + by = c$

a des solutions ssi $a \wedge b \mid c$

• $17k - 11\ell = 1$: $17 \wedge 11 = 1$

Solu° particulière : $(2,3) = (k_0, \ell_0)$

Analyse : Si (k, ℓ) solu°, alors

$17k - 11\ell = 1 = 17k_0 - 11\ell_0$

donc $17(k-k_0) = 11(\ell-\ell_0)$ $(*)$

$17 \mid 11(\ell-\ell_0)$ et $17 \wedge 11 = 1$ donc $17 \mid \ell - \ell_0$

donc on a $m \in \mathbb{Z}$ tel que $\ell = \ell_0 + 17m$.

On réinjecte dans $(*)$: $\cancel{17}(k-k_0) = 11\times\cancel{17}\times m$ et $k = k_0 + 11m$

Synthèse : $\forall m \in \mathbb{Z}$, $k = 2+11m$ et $\ell = 3+17m$ sont bien solu°.

Par équivalences : $17k - 11\ell = 1 \Leftrightarrow \begin{cases} 17 \mid 11(\ell-\ell_0) \\ 17(k-k_0) = 11(\ell-\ell_0) \end{cases} \Leftrightarrow \dots$

Puis $(S) \Leftrightarrow \exists m, n \in \mathbb{Z},\ N = 3 + 17(2+11m) = 5+6n$

18 Résoudre (S) $\begin{cases} x+\bar{5}y=\bar{8} \\ \bar{3}x+\bar{7}y=\bar{9} \end{cases}$ dans $\mathbb{Z}/13\mathbb{Z}$.

$\mathbb{Z}/13\mathbb{Z}$ corps.

$(S) \underset{L_2 \leftarrow L_2 - 3L_1}{\Leftrightarrow} \begin{cases} x+\bar{5}y=\bar{8} \\ \underbrace{-\bar{8}}_{\neq \bar{0} \text{ donc inversible}} y = \bar{9}-\bar{3}\times\bar{8} = -\overline{15} \end{cases} \Leftrightarrow \begin{cases} x+\bar{5}y=\bar{8} \\ \bar{5}y = -\bar{2} \end{cases}$

Inverse de $\bar{5}$? $\quad -5\times 5 + 2\times 13 = 1$

donc $-5\times 5 \equiv 1 \ (13)$ ou $-\bar{5}\times\bar{5}=\bar{1}$ ie $\bar{5}^{-1} = -\bar{5}$.

$(S) \Leftrightarrow \begin{cases} x+\bar{5}y=\bar{8} \\ y = -\bar{5}\times(-\bar{2}) = \overline{10} = -\bar{3} \end{cases} \Leftrightarrow \begin{cases} x = \bar{8} - \bar{5}\times y = \bar{8}+\overline{15} = \bar{8}+\bar{2} = \overline{10} = -\bar{3} \\ y = -\bar{3} \end{cases}$

Unique solu° : $(-\bar{3}, -\bar{3})$.

$-\bar{3} - \overline{15} = -\overline{18} = -\bar{5} = \bar{8}$.

$-\bar{9} - \overline{21} = \bar{4}+\bar{5} = \bar{9}$.

$\begin{pmatrix} \bar{1} & \bar{5} \\ \bar{3} & \bar{7} \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/13\mathbb{Z})$

$\begin{vmatrix} \bar{1} & \bar{5} \\ \bar{3} & \bar{7} \end{vmatrix} = \bar{7} - \bar{3}\times\bar{5} = \bar{7}-\bar{2} = \bar{5} \neq \bar{0}$.

Variante : $\begin{cases} x+\bar{5}y=\bar{8} \\ \bar{5}y = -\bar{2} \end{cases}$ dans $\mathbb{Z}/10\mathbb{Z}$??

$5 \wedge 10 \neq 1$

$\bar{5}$ non inversible.

Pas de solution.

y	$-\bar{4}$	$-\bar{3}$	$-\bar{2}$	$-\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{5}y$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$

eh oui ! modulo 10 = chiffre des unités.

$\begin{vmatrix} \bar{1} & \bar{5} \\ \bar{0} & \bar{5} \end{vmatrix} = \bar{5} \neq \bar{0}$ mais $\mathbb{Z}/10\mathbb{Z}$ n'est pas un corps...

21 Résolution d'une équation du second degré dans $\mathbb{Z}/p\mathbb{Z}$

1. Résoudre l'équation
$$x^2 - \overline{13}x + \overline{8} = \overline{0}$$
dans $\mathbb{Z}/17\mathbb{Z}$.
(On essayera de suivre la même démarche que sur $\mathbb{R}$: mise sous forme canonique… reprendre donc la démarche suivie dans le cours de première)

2. Résoudre l'équation
$$x^2 - \overline{2}x + \overline{4} = 0$$
dans $\mathbb{Z}/26\mathbb{Z}$.

1. $\mathbb{Z}/17\mathbb{Z}$ corps car 17 premier.

$$x^2 - \overline{13}\,x + \overline{8} = x^2 + \overline{4}x + \overline{8} = (x+\overline{2})^2 + \overline{4}$$
$$= (x+\overline{2})^2 - \overline{13}$$

Carrés dans $\mathbb{Z}/17\mathbb{Z}$:

y	$\overline{0}$	$\pm\overline{1}$	$\pm\overline{2}$	$\pm\overline{3}$	$\pm\overline{4}$	$\pm\overline{5}$	$\pm\overline{6}$	$\pm\overline{7}$	$\pm\overline{8}$
y^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{8}$	$-\overline{1}$	$\overline{8}$	$\overline{2}$	$-\overline{2}$	$-\overline{4} = \overline{13}$

$$x^2 - \overline{13}\,x + \overline{8} = (x+\overline{2})^2 - \overline{8}^2 = (x+\overline{2}-\overline{8})(x+\overline{2}+\overline{8})$$
$$= (x-\overline{6})(x+\overline{10})$$

$x^2 - \overline{13}\,x + \overline{8} = 0 \iff x \in \{\overline{6}, -\overline{10} = \overline{7}\}$ car $\mathbb{Z}/17\mathbb{Z}$ corps donc intègre.

2. $\mathbb{Z}/26\mathbb{Z}$ n'est pas un corps.

$(E)\ x^2 - \overline{2}x + \overline{4} = \overline{0}$ $\qquad$ On peut tester toutes les valeurs (26 …)
$$\overset{\shortparallel}{(x-\overline{1})^2 + \overline{3}}$$

$k \in \mathbb{Z}$ tels que $k^2 - 2k + 4 \equiv 0\ [26]$ ie $26 \mid k^2 - 2k + 4$

ie $k^2 - 2k + 4$ divisible par 2 et 13 car $2 \wedge 13 = 1$.

Dans $\mathbb{Z}/2\mathbb{Z}$: $(E) \iff x^2 = \overline{0} \iff x = \overline{0}$ car $\mathbb{Z}/2\mathbb{Z}$ corps.

Dans $\mathbb{Z}/13\mathbb{Z}$: $(E) \iff (x-\overline{1})^2 + \overline{3} = 0 \iff (x-\overline{1})^2 - \overline{6}^2 = \overline{0}$

y	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
y^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$-\overline{4}$	$\overline{3}$	$-\overline{1}$	$-\overline{3}$

$\iff (x-\overline{1}-\overline{6})(x-\overline{1}+\overline{6}) = \overline{0}$

$\iff x \in \{\overline{7}, \underset{\overline{8}}{\underset{\shortparallel}{-\overline{5}}}\}$ car $\mathbb{Z}/13\mathbb{Z}$ corps.

Solu° de (E) dans $\mathbb{Z}/26\mathbb{Z}$: $\overline{k}$ avec $\begin{cases} k \equiv 0\ [2] \\ k \equiv 7\ [13] \text{ ou } k \equiv 8\ [13] \end{cases}$ ie $\begin{cases} k \equiv 0\ (2) \\ k \equiv 7\ (13) \end{cases}$ ou $\begin{cases} k \equiv 0\ (2) \\ k \equiv 8\ (13) \end{cases}$

$(-6 \times 2 + 1 \times 13 = 1)$ $\qquad$ ie $\begin{cases} k \equiv 20\ [26] \\ \text{ou} \\ k \equiv 8\ [26] \end{cases}$ par thm chinois

ie $\overline{8}$ et $\overline{20} = -\overline{6}$.

20 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

1. Faire la liste des éléments de $\mathbb{Z}/17\mathbb{Z}$ qui sont des carrés. Combien y-en-a-t-il ?
2. Soit p un nombre premier impair. On note A l'ensemble des carrés dans $\mathbb{Z}/p\mathbb{Z}$: $x \in A \iff \exists y \in \mathbb{Z}/p\mathbb{Z},\ x = y^2$.
   (a) Déterminer le nombre d'éléments de A.
   (b) Démontrer que, si a est un élément non nul de A, $x \mapsto xa$ est une bijection de A sur lui-même.
   (c) Démontrer que, si a est un élément de $\mathbb{Z}/p\mathbb{Z} \setminus A$, $x \mapsto xa$ est une bijection de $A \setminus \{0\}$ sur $\mathbb{Z}/p\mathbb{Z} \setminus A$.

1. Carrés dans $\mathbb{Z}/17\mathbb{Z}$: $\bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{4}, \pm\bar{8}$ soit 9 carrés.

$k \in [\![0;8]\!]$ $\qquad \frac{17+1}{2} = 9.$

2 a) p premier impair $\quad A = \{y^2 ;\ y \in \mathbb{Z}/p\mathbb{Z}\}$

$|A|$??

Si $y, z \in \mathbb{Z}/p\mathbb{Z}$, $y^2 = z^2 \Leftrightarrow y^2 - z^2 = \bar{0} \Leftrightarrow (y-z)(y+z) = \bar{0}$

$\Leftrightarrow y = \pm z$ car $\mathbb{Z}/p\mathbb{Z}$ corps (intègre).

p premier (impair)

Il suffit de calculer $\bar{k}^2$ avec $k \in [\![0, \frac{p-1}{2}]\!]$

donc $|A| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$. $\qquad |[\![a;b]\!]| = b - a + 1$.

b) bien définie, exhiber une réciproque.

c) idem.

25 Quels sont les sous-groupes finis de $(\mathbb{C}^*, \times)$?

Analyse : Soit G sous-groupe fini de $(\mathbb{C}^*, \times)$. $\quad$ exemple : $\{1\} = \mathbb{U}_1$, $\{\pm 1\} = \mathbb{U}_2$, $\mathbb{U}_n$.

$n = |G|$. But : $G = \mathbb{U}_n = \{z \in \mathbb{C} ;\ z^n = 1\}$

Soit $z \in G$, z d'ordre fini car G fini

et son ordre divise $n = |G|$.

donc $z^{|G|} = z^n = 1$. donc $z \in \mathbb{U}_n$.

donc $G \subset \mathbb{U}_n$.

et $|G| = |\mathbb{U}_n| = n$ donc $\mathbb{U}_n$.

Synthèse : les $\mathbb{U}_n$ ss-gpes finis de $(\mathbb{C}^*, \times)$: cours.

Il n'y en a pas d'autres.

22 **Théorème de Wilson (un test de primalité)**

1. Montrer que si $(p-1)! \equiv -1\ [p]$, alors p est premier.
2. Réciproquement, on suppose que p est premier. En rassemblant les termes du produit par paires, justifier que $(p-1)! \equiv -1\ [p]$.

1 – Si $(p-1)! \equiv -1\ (p)$, on a $k \in \mathbb{Z}$ tel que

$(p-1)! = 2 \times 3 \times \dots \times (p-1) = -1 + kp$. Alors aucun des entiers entre 2 et $p-1$ ne peut diviser p (il diviserait 1) donc p est premier.

2 – Si p premier, $(p-1)! = \prod_{k=1}^{p-1} k$

dans $\mathbb{Z}/p\mathbb{Z}$: $\prod_{\substack{x \in \mathbb{Z}/p\mathbb{Z} \\ x \neq \bar{0}}} x = \prod_{x \in U_{\mathbb{Z}/p\mathbb{Z}}} x$ car $\mathbb{Z}/p\mathbb{Z}$ corps. <u>But</u> : ... $= -\bar{1}$.

On rassemble chaque élément avec son inverse ... quand c'est possible.
(commutatif...) ie si $x \neq x^{-1}$

Or $x = x^{-1} \iff x^2 = \bar{1} \iff x^2 - \bar{1}^2 = \bar{0} \iff (x - \bar{1})(x + \bar{1}) = \bar{0}$
$\iff x = \pm \bar{1}$ car $\mathbb{Z}/p\mathbb{Z}$ corps

$\overline{(p-1)!} = \bar{1} \times (-\bar{1}) \times \underbrace{\bar{1}}_{\text{termes associés avec leur inverse}} = -\bar{1}$ donc $(p-1)! \equiv -1\ (p)$.