Tableau

1 Séance 19 oct 2020

Exercice. (TD2 Ex6.2) Donner un exemple de 10 entiers consécutifs non premiers.

Soient $n \in \mathbb{N}_{>0}$, $N := n!$. alors pour $2 \leq k \leq n$, on a $k \mid N + k$, donc $N + k$ est non-premier. En utilisant ce résultat, on a $n = 11$, alors $11! + 2, \cdots, 11! + 11$ sont non-premiers.

Exercice. (TD2 Ex7) Calculer $\mathrm{pgcd}(195, 143)$ et $\mathrm{ppcm}(195, 143)$. En utilisant l'algorithme d'Euclide.

Réponse.

$$\begin{aligned} 195 &= 1 \times 143 + 52 \\ 143 &= 2 \times 52 + 39 \\ 52 &= 1 \times 39 + 13 \\ 39 &= 3 \times 13 \end{aligned}$$

Donc $\mathrm{pgcd}(195.143) = 13$.

En effet, par l'Ex12 de TD2, on a $\mathrm{ppcm}(195, 143) = 195 \times 143 / \mathrm{pgcd}(195.143) = 195 \times 143 / 13$,

Maintenant, $195/13 = 15 \Longrightarrow 195 = 13 \times 15 = 3 \times 5 \times 13$. $143 = 13 \times 11$, alors on a $\mathrm{ppcm}(195, 143) = 3 \times 5 \times 11 \times 13$ par la formule de ppcm.

Remarque 1. On peut utiliser l'algorithme d'Euclide pour faciliter la factorisation.

Remarque 2. En effet, l'algorithme d'Euclide ($\sim \log(\max(m, n))$) est beaucoup plus efficace que la factorisation ($\sim \sqrt{\max(m, n)}$) pour calculer $\mathrm{ppgcd}(m, n)$ quand $m, n \gg 0$ pour les ordinateurs.

Exercice. (TD2 Ex8) Trouver $d = \mathrm{pgcd}(36, 126)$ et une relation $36\,a + 126\,b = d$ en utilisant l'algorithme d'Euclide.

Réponse.

$$\begin{aligned} 126 &= 3 \times 36 + 18 \\ 36 &= 2 \times 18 \end{aligned} \tag{1}$$

Donc $d = 18$. Par (1), on a $18 = 36 \times (-3) + 126 \times 1$, donc on peut prendre $a = -3 =: a_0$ et $b = 1 = b_0$.

Chercher tous les $(a, b) \in \mathbb{Z}^2$ t.q. $36\,a + 126\,b = d \iff \frac{36}{d}\,a + \frac{126}{d}\,b = 1$ où $\mathrm{pgcd}(36/d, 126/d) = 1$ (en effet, $36/d = 2$ et $126/d = 7$).

Donc on a $\frac{36}{d}\,a + \frac{126}{d}\,b = 1 = \frac{36}{d}\,a_0 + \frac{126}{d}\,b_0 \Longrightarrow \frac{36}{d}\,(a - a_0) = \frac{126}{d}\,(b_0 - b) \Longrightarrow \frac{126}{d} \mid a - a_0$. On prend $t \in \mathbb{Z}$ t.q. $a - a_0 = \frac{126}{d}\,t$, on a $b - b_0 = -\frac{36}{d}\,t$

En résumé, $a = a_0 + \frac{126}{d}\,t$ et $b = b_0 - \frac{36}{d}\,t$.

Remarque 3. Pour résoudre une équation $a\,x + b\,y = c$ où $a, b, c, x, y \in \mathbb{Z}$

1. Calculer $d = \mathrm{pgcd}(a, b)$ (par l'algorithme d'Euclide)
2. Si $d \nmid c$, aucune solutions. Sinon, on a $a_0\,x + b_0\,y = c_0$, où $a_0 = a/d \in \mathbb{Z}, b_0 = b/d \in \mathbb{Z}, c_0 = c/d \in \mathbb{Z}$
3. Par l'algorithme d'Euclide, on a trouvé $(x_0, y_0) \in \mathbb{Z}$ t.q. $a_0 x_0 + b_0\,y_0 = 1$, donc $(c_0\,x_0, c_0\,y_0)$ est une solution de $a\,x + b\,y = c$.
4. En général, les solutions sont $(x, y) = (x_0 + b_0\,t, y_0 - a_0\,t)$ où $t \in \mathbb{Z}$.

Exercice. (TD2 Ex9) Résoudre dans $\mathbb{Z}^2$ les équations suivantes: $4x+9y=1$, $18x+7y=2$, $5x-18y=4$, $6x+15y=28$, $56x+35y=14$

Réponse. Tout d'abord, nous essayons de résoudre $6x+15y=28$. $3=\text{pgcd}(6,15)\nmid 28$ donc aucune solution.

Pour $4x+9y=1$, une solution particulière $(x,y)=(-2,1)$. Toutes les solutions: $(x,y)=(-2+9t,1-4t), t\in\mathbb{Z}$.

2 Séance 21 oct 2020

Exercice. (TD2 Ex9) Résoudre dans $\mathbb{Z}^2$ les équations suivantes: $18\,x+7\,y=2$, $5\,x-18\,y=4$, $56\,x+35\,y=14$

Réponse. Pour $56\,x+35\,y=14$, on utilise l'algorithme d'Euclide

$$\begin{aligned} 56 &= 1\times 35+21\\ 35 &= 1\times 21+14\\ 21 &= 1\times 14+7\\ 14 &= 2\times 7 \end{aligned}$$

Donc $\mathrm{pgcd}(56,35)=7$.

$$\begin{aligned} 8 &= 1\times 5+3 &(2)\\ 5 &= 1\times 3+2 &(3)\\ 3 &= 1\times 2+1 &(4) \end{aligned}$$

Alors on a $1\overset{(4)}{=\!=}3-1\times 2\overset{(3)}{=\!=}3-1\times(5-1\times 3)=(-1)\times 5+2\times 3\overset{(2)}{=\!=}(-1)\times 5+2\times(8-1\times 5)=2\times 8-3\times 5$

Donc $56\,x+35\,y=14$ admet une solution $(x,y)=(2\,2,2\,(-3))=(4,-6)$. La solution générale $(x,y)=(4+5\,t,-6-8\,t)$ où $t\in\mathbb{Z}$

Ici $a_0=8, b_0=5, c_0=14/7=2$

Pour $18\,x+7\,y=2$,

$$\begin{aligned} 18 &= 2\times 7+4\\ 7 &= 2\times 4-1 \end{aligned}$$

Remarque 4. Pour $a=b\,q+r$, vous pouvez remplacer le reste $r\in[0,b[$ par $r\in[-E(b/2),E(-b/2)+b[$

Alors $1=2\times 4-7=2\times(18-2\times 7)-7=2\times 18-5\times 7$

On trouve une solution particulière $(x,y)=(4,-10)$. La solution générale: $(4+7\,t,-10-18\,t)$ pour $t\in\mathbb{Z}$.

Remarque 5. Si on remplace t par $c\,t+d$ où $c=\pm 1, d\in\mathbb{Z}$, $(4+5\,t,-6-8\,t)\leftarrow(4+5\,(c\,t+d),-6-8\,(c\,t+d))=(5\,c\,t+5\,d+4,-8\,c\,t-8\,d-6)$

Remarque 6.

$$\begin{aligned} r_{n-2} &= r_{n-1}\,q_{n-1}+r_n\\ r_{n-3} &= r_{n-2}\,q_{n-2}+r_{n-1}\\ r_{n-4} &= r_{n-3}\,q_{n-3}+r_{n-2} \end{aligned}$$

Alors $r_n=-q_{n-1}\,r_{n-1}+r_{n-2}=-q_{n-1}\,(r_{n-3}-q_{n-2}\,r_{n-2})=q_{n-1}\,q_{n-2}\,r_{n-2}-q_{n-1}\,r_{n-3}=q_{n-1}\,q_{n-2}\,(r_{n-4}-q_{n-3}\,r_{n-3})-q_{n-1}\,r_{n-3}=-q_{n-1}\,(1+q_{n-2}\,q_{n-3})\,r_{n-3}+q_{n-1}\,q_{n-2}\,r_{n-4}=\cdots$ (les formules pour la fraction continuée)

$$\begin{aligned} \begin{pmatrix} r_n\\ r_{n-1}\end{pmatrix} &= A_{n-1}\begin{pmatrix} r_{n-1}\\ r_{n-2}\end{pmatrix}\\ &= A_{n-1}\,A_{n-2}\begin{pmatrix} r_{n-2}\\ r_{n-3}\end{pmatrix}\\ &= \cdots\\ &= A_{n-1}\,A_{n-2}\cdots\begin{pmatrix} a\\ b\end{pmatrix} \end{aligned}$$

où $A_n=\begin{pmatrix} 1 & *\\ 1 & \end{pmatrix}$

3 Séance 26 oct 2020

Exercice. (TD2 Ex10) Soient $a, b, x, y \in \mathbb{Z}$ $(a, b \neq 0)$. Montrer que si l'entier $d = a\,x + b\,y > 0$ divise a et b alors $d = \mathrm{pgcd}(a, b)$.

Réponse. Pour $(a, b) \in \mathbb{Z} \setminus \{0\}$, la définition de $\mathrm{pgcd}(a, b)$: un entier positif $e > 0$ t.q.

1. $e \mid a$, $e \mid b$;
2. Pour tout $f \in \mathbb{Z}$ t.q. $f \mid a$, $f \mid b$, alors on a $f \mid e$.

Il suffit de vérifier que d satisfait les énoncés pou e au-dessus.

Exercice. (TD2 Ex11) Soient $a, b, c, d \in \mathbb{Z} \setminus \{0\}$. Montrer que

1. $\text{pgcd}(a, b) = d \Longrightarrow \text{pgcd}(a\,c, b\,c) = d\,|c|$.
2. $(\text{pgcd}(a, b) = 1 \ \text{ et } \ \text{pgcd}(a, c) = 1) \Longrightarrow \text{pgcd}(a, b\,c) = 1$.
3. $\text{pgcd}(a, b) = 1 \Longrightarrow (\forall m, n \geq 2 : \text{pgcd}(a^m, b^n) = 1)$.
4. $\text{pgcd}(a, b) = d \Longrightarrow (\forall m \geq 2 : \text{pgcd}(a^m, b^m) = d^m)$.

Réponse.

1. Il suffit de montrer que
   a. $d\,|c|$ divise $a\,c$ et $b\,c$
   b. si e divise $a\,c \ \text{ et } \ b\,c$ alors e divise $d\,|c|$ (Bézout: $d = a\,x + b\,y$).
2. Il suffit de montrer que pour tout premier $p \,|\, a$, on a $p \nmid b\,c$. $\text{pgcd}(a, b) = 1 \Longrightarrow p \nmid b$. p ne divise pas c. Donc $p \nmid b\,c$.

   Alternativement, vous pouvez utiliser l'identité d'Euclide.
3. Méthode 1: par récurrence sur m et n. Méthode 2: Pour tout $p \,|\, a^m$, p divise a alors p ne divise pas b, donc p ne divise pas b^n.
4. $\text{pgcd}(a/d, b/d) = 1 \Longrightarrow \text{pgcd}((a/d)^m, (b/d)^m) = 1 \Longrightarrow \text{pgcd}(a^m, b^m) = d^m$.

4 Séance 28 oct 2020

Question. (CC1) Soient $n>1$ un entier et $p\neq q$ deux nombres premiers distincts. Montrer que la racine n-ième $\sqrt[n]{p\,q}\notin\mathbb{Q}$.

Réponse. Sinon, $r=(p\,q)^{1/n}\in\mathbb{Q}$, alors $r^n=p\,q\Longrightarrow n\,v_p(r)=v_p(p\,q)=v_p(p)+v_p(q)=1\Longrightarrow v_p(r)=1/n\notin\mathbb{Z}$.

Question. (CC1) Soient $n\in\mathbb{N}_{>0}$ et $a,b\in\mathbb{Z}\setminus\{0\}$. Montrer que si $a^{n+1}\,|\,b^n$, alors on a $a\,|\,b$.

Réponse. $a^{n+1}\,|\,b^n$ implique que pour tout premier p, $(n+1)\,v_p(a)\leq n\,v_p(b)\Longrightarrow v_p(a)\leq n\,v_p(b)/(n+1)\leq v_p(b)$, donc $a\,|\,b$.

Question. (CC2) Calculer $\mathrm{pgcd}(a,b),\mathrm{ppcm}(a,b)$ et résoudre l'équation $a\,x+b\,y=c$ pour $(x,y)\in\mathbb{Z}^2$ où $a=68$, $b=42$ et $c=12$ (Il n'est pas nécessaire d'évaluer $\mathrm{ppcm}(a,b)$ dont une factorisation suffit).

Réponse. Calculons $\mathrm{pgcd}(a,b)$ par l'algorithme d'Euclide,

$$\begin{aligned}
68 &= 1\times 42+26\\
42 &= 1\times 26+16\\
26 &= 1\times 16+10\\
16 &= 1\times 10+6\\
10 &= 1\times 6+4\\
6 &= 1\times 4+2\\
4 &= 2\times 2
\end{aligned}$$

Donc $\mathrm{pgcd}(a,b)=2$. $\mathrm{ppcm}(a,b)=68\times 42/2$

Pour résoudre l'équation $a\,x+b\,y=c$, tout d'abord, $\mathrm{pgcd}(a,b)\,|\,c$.

$$\begin{aligned}
2 &= 1\times 6-1\times 4\in 4\,\mathbb{Z}+6\,\mathbb{Z}\\
&= 1\times 6-1\times(10-1\times 6)\\
&= 2\times 6-1\times 10\in 6\,\mathbb{Z}+10\,\mathbb{Z}\\
&= 2\times(16-10)-1\times 10\\
&= 2\times 16-3\times 10\in 10\,\mathbb{Z}+16\,\mathbb{Z}\\
&= 2\times 16-3\times(26-16)\\
&= -3\times 26+5\times 16\in 16\,\mathbb{Z}+26\,\mathbb{Z}\\
&= -3\times 26+5\times(42-26)\\
&= 5\times 42-8\times 26\in 26\,\mathbb{Z}+42\,\mathbb{Z}\\
&= 5\times 42-8\times(68-42)\\
&= -8\times 68+13\times 42\in 42\,\mathbb{Z}+68\,\mathbb{Z}
\end{aligned}$$

Donc en multipliant 6, on obtient une solutions particulière: $(x,y)=(-48,78)$. La solution générale: $(x,y)=(-48+21\,t,\,78-34\,t)$.

Question. (TD3 Ex4.bc) Résoudre dans $\mathbb{Z}$:

1. $10\,x \equiv 6 \pmod{14}$
2. $\begin{cases} 7\,x \equiv 5 \pmod{19} \\ 6\,x \equiv 3 \pmod{15} \end{cases}$

Réponse.

1. L'équation $a\,x \equiv c \pmod{b}$: $a\,x - b\,y = c$. En général,
   a. Calculer $d := \mathrm{pgcd}(a, b)$. Si $d \nmid c$, aucune solution.
   b. Sinon, il suffit de résoudre l'équation $\frac{a}{d}\,x \equiv \frac{c}{d} \left(\mathrm{mod}\, \frac{b}{d}\right)$. On utilise l'algorithme d'Euclide pour chercher un inverse de $\frac{a}{d} \left(\mathrm{mod}\, \frac{b}{d}\right)$: posons $a_1 := a/d$, $b_1 := b/d$ et $c_1 := c/d$. si vous trouvez $u, v \in \mathbb{Z}$ t.q. $a_1\,u + b_1\,v = 1$, alors $a_1\,u \equiv 1 \pmod{b_1}$, donc u est un inverse.
   c. $a_1\,x\,u \equiv c_1\,u \pmod{b_1} \Longrightarrow x \equiv c_1\,u \pmod{b_1}$.

   En particulier,
   a. $14 = 1 \times 10 + 4, 10 = 2 \times 4 + 2, 4 = 2 \times 2$, donc $\mathrm{pgcd}(10, 14) = 2$.
   b. $5\,x \equiv 3 \pmod{7}$. $2 = 10 - 2 \times 4 = 10 - 2 \times (14 - 1 \times 10) = -2 \times 14 + 3 \times 10$. Donc $1 = -2 \times 7 + 3 \times 5$, alors $3 \times 5 \equiv 1 \pmod{7}$.
   c. $x \equiv 3 \times 3 \equiv 2 \pmod{7}$
2. En résolvant les équations, le système est équivalent à $\begin{cases} x \equiv -2 (\mathrm{mod}\, 19) \\ x \equiv -2 (\mathrm{mod}\, 5) \end{cases}$ donc $x \equiv -2 \pmod{95 = \mathrm{ppcm}(19, 5)}$

   Remarque 7. En général, pour résoudre un système d'équations $\begin{cases} x \equiv c_1 \pmod{a_1} \\ x \equiv c_2 \pmod{a_2} \end{cases}$, $x = a_1\,y + c_1 = a_2\,z + c_2$ où $y, z \in \mathbb{Z}$, il suffit de résoudre $a_1\,y + c_1 = a_2\,z + c_2 \Rightarrow a_1\,y - a_2\,z = c_2 - c_1$. En particulier, alors la solution générale s'écrit comme $x \equiv (\mathrm{mod}\, \mathrm{ppcm}(a_1, a_2))$.

   Pour un système

$$\begin{cases} x \equiv c_1 \pmod{a_1} \\ x \equiv c_2 \pmod{a_2} \\ \cdots \\ x \equiv c_n \pmod{a_n} \end{cases}$$

   où $\mathrm{pgcd}(a_i, a_j) = 1$ pour tout $i \neq j$ (il suffit de résoudre le système avec $(c_1, \ldots, c_n) = (0, \ldots, 0, 1, 0, \ldots, 0)$, par exemple, $c_1 = 1$ et $c_2 = \cdots = c_n = 0$, alors il est équivalent à $\begin{cases} x \equiv 1 \pmod{a_1} \\ x \equiv 0 \pmod{a_2 \cdots a_n} \end{cases}$. Pour les $(c_1, \ldots, c_n)$, il suffit de faire une combinaison linéaire des solutions pour $(c_1, \ldots, c_n) = (0, \ldots, 0, 1, 0, \ldots, 0)$.

Question. $\mathrm{pgcd}(a,b)=d \Longrightarrow \big(\forall m,n\geq 2\colon \mathrm{pgcd}\big(\frac{a^m}{d^m},\frac{b^n}{d^n}\big)=1\big)$.

Réponse. $a=a_1\,d, b=b_1\,d$ alors $\mathrm{pgcd}(a_1,b_1)=1$. Donc $\mathrm{pgcd}(a_1^m,b_1^n)=1$.

Exercice. (TD2 Ex12) Soient $a, b \in \mathbb{Z}$. Montrer que $\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b) = |a\,b|$.

Réponse. Il suffit de vérifier que pour tout premier p, on a $v_p(\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b)) = v_p(|a\,b|) = v_p(a\,b)$. En effet, $v_p(\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b)) = v_p(\operatorname{pgcd}(a,b)) + v_p(\operatorname{ppcm}(a,b)) = \min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b) = v_p(a\,b)$.

Question. (TD3 Ex1) $a = \sum_{j=0}^{r} a_j \times 10^j$. Montrer que

1. 3 divise a ssi 3 divise $\sum_{j=0}^{r} a_j$
2. 9 divise a ssi 9 divise $\sum_{j=0}^{r} a_j$
3. 11 divise a ssi 11 divise $\sum_{j=0}^{r} (-1)^j a_j$

Réponse.

1. $a \equiv \sum_{j=0}^{r} a_j \pmod 3$
2. Similaire
3. $10 \equiv -1 \pmod{11}$ donc $a \equiv \sum_{j=0}^{r} (-1)^j a_j$

5 Séance 2 nov 2020

Question. (TD3 Ex7) Trouver $100^{1000} \bmod 13$ [Indication $x^{12} \equiv 1 \pmod{13}$ pour $x \not\equiv 0 \pmod{13}$].

Réponse. $1000/12 = 500/6 = 250/3 \in \mathbb{Z} + 1/3$ donc le reste est $1/3 \times 12 = 4$. Donc $100^{1000} \equiv 100^4 \pmod{13}$, ensuite $100/13 \in \mathbb{Z} + 9/13 = \mathbb{Z} - 4/13$ donc le reste est -4. Alors $100^{1000} \equiv 100^4 \equiv (-4)^4 \equiv 16^2 \equiv 3^2 \equiv -4 (\bmod 13)$.

Question. (TD3 Ex8) Montrer que $13 \mid 2^{70} + 3^{70}$.

Réponse. Il suffit de calculer $2^{70} \bmod 13$ et $3^{70} \bmod 13$. $70/12 = 35/6 \in \mathbb{Z} - 1/6$ donc le reste est -2. Donc $2^{70} \equiv 2^{-2} \equiv 7^2 \equiv -3 \pmod{13}$ et $3^{70} \equiv 3^{-2} \equiv (-4)^2 \equiv 3 \pmod{13}$, donc $2^{70} + 3^{70} \equiv 0 \pmod{13}$.

6 Séance 4 nov 2020

Algorithme d'Euclide Pour $(a,b)\in\mathbb{Z}^2$ où $b\neq 0$, on a

$$\begin{array}{rcl|rcl}
a & = & b\,q_1+r_1 & r_1 & = & a-b\,q_1=a\,s_1+b\,t_1\in a\,\mathbb{Z}+b\,\mathbb{Z}\\
b & = & r_1\,q_2+r_2 & r_2 & = & b-r_1\,q_2=b-(a\,s_1+b\,t_1)\,q_2=a\,s_2+b\,t_2\in a\,\mathbb{Z}+b\,\mathbb{Z}\\
r_1 & = & r_2\,q_3+r_3 & r_3 & = & r_1-r_2\,q_3=(a\,s_1+b\,t_1)-(a\,s_1+b\,t_1)\,q_3=a\,s_3+b\,t_3\in a\,\mathbb{Z}+b\,\mathbb{Z}\\
r_2 & = & r_3\,q_4+r_4 & r_4 & = & r_2-r_3\,q_4=(a\,s_2+b\,t_2)-(a\,s_3+b\,t_3)\,q_4=a\,s_4+b\,t_4\in a\,\mathbb{Z}+b\,\mathbb{Z}\\
 & \vdots & & & & \\
r_{n-2} & = & r_{n-1}\,q_n+r_n & r_n & = & r_{n-2}-r_{n-1}\,q_n=(a\,s_{n-2}+b\,t_{n-2})-(a\,s_{n-1}+b\,t_{n-1})\,q_n=a\,s_n+b\,t_n\in a\,\mathbb{Z}+b\,\mathbb{Z}\\
r_{n-1} & = & r_n\,q_{n+1} & & &
\end{array}$$

Cela veut dire que nous écrivons $a,b,r_1,\ldots,r_n$ consécutivement comme des combinaisons linéaires de a,b. Alors $r_n=\mathrm{pgcd}(a,b)$, et que $r_n=a\,s_n+b\,t_n$, une relation de Bézout.

C'est « meilleur » que ce que je vous ai affiché avant à point de vue informatique: la complexité en espace est constante.

Question. (TD3 Ex2) Soient $x, y, z \in \mathbb{Z}$. Montrer que

1. $x^2 \equiv 0, 1 \pmod 3$
2. Si $3 \mid (x^2 + y^2)$, alors $3 \mid x$ et $3 \mid y$.
3. Si $x^2 + y^2 = 3\,z^2$, alors $3 \mid x, 3 \mid y \text{ et } 3 \mid z$.
4. Si $x^2 + y^2 = 3\,z^2$,alors $x = y = z = 0$.
5. Que se passe-t-il si l'on remplace 3 par 5 (resp. par 7)?

Réponse.

1. Soit $x \equiv 0, \pm 1 \pmod 3$, $x^2 \equiv 0, 1 \pmod 3$ (énumérer toutes les possibilités)
2. Énumérer $x^2 \equiv 0, 1$ ou $y^2 \equiv 0, 1$. D'autant que $x^2 + y^2 \equiv 0$, la seule possibilité: $x^2 \equiv 0$ et $y^2 \equiv 0$, donc $x \equiv y \equiv 0$.
3. $x^2 + y^2 = 3\,z^2$ alors $3 \mid (x^2 + y^2) \Longrightarrow 3 \mid x \text{ et } 3 \mid y \Longrightarrow 9 \mid (x^2 + y^2) \Longrightarrow 9 \mid (3\,z^2) \Longrightarrow 3 \mid z^2 \xRightarrow{\text{(3 est premier)}} 3 \mid z$.
4. Il suffit de montrer que

   Lemme 8. *Pour tout $n \in \mathbb{N}$, on a $3^n \mid x, 3^n \mid y \text{ et } 3^n \mid z$.*

   Tout d'abord, pourquoi c'est suffisant, c'est-à-dire, si pour tout $n \in \mathbb{N}$, on a $3^n \mid x$, alors $x = 0$.

   On peut montre Lemme 8 par récurrence. Tout d'abord, quand $n = 0$, c'est tautologie. Supposons que $3^m \mid x, y \text{ et } z$, alors on prend $x = 3^m x_1, y = 3^m y_1, z = 3^m z_1$ ou $x_1, y_1, z_1 \in \mathbb{Z}$. Alors $x^2 + y^2 = 3\,z^2 \Longrightarrow x_1^2 + y_1^2 = 3\,z_1^2$. Ensuite, par la question précédente, on a $3 \mid x_1, y_1 \text{ et } z_1$, donc $3^{m+1} \mid x, y \text{ et } z$.
5. Pour 5, c'est faux: $1^2 + 2^2 = 5 \times 1^2$. Pour 7, c'est vrai dont le raisonnement est similaire au cas de 3.

Question. *En utilisant l'algorithme d'Euclide*, résoudre dans $\mathbb{Z}$ les systèmes d'équations

$$\begin{cases} x & \equiv & 1 & (\mathrm{mod}\, 34) \\ x & \equiv & 0 & (\mathrm{mod}\, 55) \end{cases}$$

et

$$\begin{cases} x & \equiv & 0 & (\mathrm{mod}\, 34) \\ x & \equiv & 1 & (\mathrm{mod}\, 55) \end{cases}$$

[Indication: on peut résoudre les deux systèmes d'équations en même temps.]

En déduire la solution de

$$\begin{cases} x & \equiv & \alpha & (\mathrm{mod}\, 34) \\ x & \equiv & \beta & (\mathrm{mod}\, 55) \end{cases}$$

pour tout $(\alpha, \beta) \in \mathbb{Z}^2$.

Remarque. $x \equiv 0\,(\mathrm{mod}\, 55)$ c'est équivalent à, par exemple, $x = 55\,y$ où $y \in \mathbb{Z}$, alors la première équation est essentiellement équivalente à $55\,y \equiv 1\,(\mathrm{mod}\, 34)$.

Réponse. Tout d'abord, on utilise l'algorithme d'Euclide:

$$\begin{array}{rcl|rcl} 55 & = & 34+21 & 21 & = & 55-34 \\ 34 & = & 21+13 & 13 & = & 34-21 = 34-(55-34) = -55+2\times 34 \\ 21 & = & 13+8 & 8 & = & 21-13 = (55-34)-(-55+2\times 34) = 2\times 55-3\times 34 \\ 13 & = & 8+5 & 5 & = & 13-8 = (-55+2\times 34)-(2\times 55-3\times 34) = -3\times 55+5\times 34 \\ 8 & = & 5+3 & 3 & = & 8-5 = (2\times 55-3\times 34)-(-3\times 55+5\times 34) = 5\times 55-8\times 34 \\ 5 & = & 3+2 & 2 & = & 5-3 = (-3\times 55+5\times 34)-(5\times 55-8\times 34) = -8\times 55+13\times 34 \\ 3 & = & 2+1 & 1 & = & 3-2 = (5\times 55-8\times 34)-(-8\times 55+13\times 34) = 13\times 55-21\times 34 \\ 2 & = & 2\times 1 & & & \end{array}$$

Donc la relation de Bézout: $1 = 13\times 55 - 21\times 34$ et $\mathrm{pgcd}(34, 55) = 1$, donc les systèmes admettent une seule solution $(\mathrm{mod}\, 34\times 55)$, et $13\times 55 \equiv 1\,(\mathrm{mod}\, 34)$ et $13\times 55 \equiv 0\,(\mathrm{mod}\, 55)$ donc $x \equiv 13\times 55\,(\mathrm{mod}\, 34\times 55)$ est une solution du premier système (vous pouvez voir que les étapes ici sont parallèles à celles de $55\,y \equiv 1\,(\mathrm{mod}\, 34)$: 13 est l'inverse de $55 \bmod 34$). Parallèlement, $x \equiv -21\times 34\,(\mathrm{mod}\, 34\times 55)$ est une solution du second système.

Pour la troisième, $x \equiv 13\times 55\,\alpha - 21\times 34\,\beta\,(\mathrm{mod}\, 34\times 55)$.

7 Séance 23 nov 2020

Exercice. (TD3 Ex4.a) Résoudre dans $\mathbb{Z}$

$$\begin{cases} x & \equiv & 3 & (\mathrm{mod}\, 7) \\ x & \equiv & 1 & (\mathrm{mod}\, 8) \\ x & \equiv & 4 & (\mathrm{mod}\, 9) \end{cases} \tag{5}$$

Solution. Tout d'abord, nous résolvons

$$\begin{cases} x & \equiv & 3 & (\mathrm{mod}\, 7) \\ x & \equiv & 1 & (\mathrm{mod}\, 8) \end{cases}$$

D'autant que $8-7=1$, alors $8\equiv 1\,(\mathrm{mod}\,7)$ et $8\equiv 0\,(\mathrm{mod}\,8)$; $-7\equiv 0\,(\mathrm{mod}\,7)$ et $-7\equiv 1\,(\mathrm{mod}\,8)$. La solution est $x\equiv 8\times 3+(-7)\times 1\equiv 17\,(\mathrm{mod}\,7\times 8)$.

Alors le système (5) est équivalent à

$$\begin{cases} x & \equiv & 17 & (\mathrm{mod}\, 7\times 8) \\ x & \equiv & 4 & (\mathrm{mod}\, 9) \end{cases} \tag{6}$$

Il suffit d'applique l'algorithme d'Euclide au pair $(7\times 8, 9)$.

Alternativement, on peut évaluer les inverses de $7, 8$ modulo 9: $8^{-1}\equiv(-1)^{-1}\equiv -1\,(\mathrm{mod}\,9)$. Ensuite, on applique l'algorithme d'Euclide au pair $(7,9)$:

$$\begin{aligned} 9 &= 1\times 7+2 \\ 7 &= 3\times 2+1 \end{aligned}$$

Alors $2=9-1\times 7$ et $1=7-3\times 2=7-3\,(9-1\times 7)=4\times 7-3\times 9$. Donc $4\times 7\equiv 1\,(\mathrm{mod}\,9)$, cela vaut dire, $7^{-1}\equiv 4\,(\mathrm{mod}\,9)$. Pour résoudre le système (6), on prend $x=17+7\times 8\,y$, alors on a $17+7\times 8\,y\equiv 4\,(\mathrm{mod}\,9)$, cela vaut dire $7\times 8\,y\equiv 5\,(\mathrm{mod}\,9)\Longrightarrow y\equiv 5\,(7^{-1})\,(8^{-1})\equiv 5\times 4\times(-1)\equiv -2\,(\mathrm{mod}\,9)$. Donc $x=17+7\times 8\times(9\,k-2)\equiv 17-2\times 7\times 8(\mathrm{mod}\,7\times 8\times 9)$.

Exercice. (TD3 Ex6) Enumérer les classes de congruence inversibles $a\,(\mathrm{mod}\,12)\in(\mathbb{Z}/12\,\mathbb{Z})^\times$. Pour chaque élément de l'ensemble $(\mathbb{Z}/12\,\mathbb{Z})^\times$ determiner son inverse. Idem pour $(\mathbb{Z}/18\,\mathbb{Z})^\times$.

Solution. $a\,(\mathrm{mod}\,12)\in(\mathbb{Z}/12\,\mathbb{Z})^\times$ ssi $\mathrm{pgcd}(a,12)=1$ ($12=2^2\times 3$ alors $\mathrm{pgcd}(a,12)=1$ ssi $2\nmid a$ et $3\nmid a$), c'est-à-dire, $a\equiv\pm 1,\pm 5$. Dans ce cas, $\mathrm{ppcm}(\varphi(2^2),\varphi(3))=\mathrm{ppcm}(2,2)=2$, donc pour tout tel a, on a $a^2\equiv 1\,(\mathrm{mod}\,12)$, donc $a^{-1}\equiv a\,(\mathrm{mod}\,12)$.

Parallèllement, $a\,(\mathrm{mod}\,18)\in(\mathbb{Z}/18\,\mathbb{Z})^\times$ ssi $\mathrm{pgcd}(a,18)=1$ ($18=2\times 3^2$ alors $\mathrm{pgcd}(a,18)=1$ ssi $2\nmid a$ et $3\nmid a$), c'est-à-dire, $a\equiv\pm 1,\pm 5,\pm 7\,(\mathrm{mod}\,18)$. On peut évaluer un par un $a^{-1}\,(\mathrm{mod}\,18)$. Il suffit de trouver les inverses de $1,5,7$. On utilise l'algorithme d'Euclide pour évaluer 5^{-1} et 7^{-1} modulo 18.

Problème. Calculer la fonction d'Euler $\varphi(n)$ et le reste $a^m \bmod n$.

Proposition. *Si* $n = \prod_{j=1}^{s} p_j^{r_j}$, *alors* $\varphi(n) = \prod_{j=1}^{s} (p_j - 1)\, p_j^{r_j - 1}$. *Par exemple,* $\varphi(9) = \varphi(3^2) = (3-1) \times 3^{2-1} = 6$

Exercice. (TD4 Ex4.1) Calculer $\varphi(64)$, $\varphi(125)$, $\varphi(100)$ et $\varphi(108)$.

Solution. $\varphi(64) = \varphi(2^6) = 2^5 = 32$, $\varphi(125) = \varphi(5^3) = 4 \times 5^2 = 100$, $\varphi(100) = 2 \times 4 \times 5 = 40$, $\varphi(108) = \varphi(2^2 \times 3^3) = 2 \times 2 \times 3^2 = 36$.

Cas particulier $n = p$. $a^m \bmod p$ pour $m \geq 1$

1. Si $p \mid a$, alors $p \mid a^m$, donc $a^m \equiv 0 \pmod p$.
2. Sinon, on a $a^{p-1} \equiv 1 \pmod p$. On calcule le reste $m \equiv m_0 \pmod{p-1}$. Alors $a^m \equiv a^{m_0}\, (a^{p-1})^{(m-m_0)/(p-1)} \equiv a^{m_0} \pmod p$.
3. Évaluer $a^{m_0} \bmod p$ (on peut remplacer a par le reste $a \bmod p$).

Remarque. Si nous devons calculer $a^m \bmod p$ pour tout $m \in \mathbb{N}$, il suffit de calculer $(a^m \bmod p)_{m \in \mathbb{N}}$ un par un a^0, $a^1, a^2, \ldots$ en utilisant $a^m = a^{m-1} \times a$. En particulier, si $p \nmid a$ et m_1 est le premier $m \in \mathbb{N}_{>0}$ t.q. $a^m \equiv 1 \pmod p$, alors l'*ordre* de $a \pmod p$ est m_1.

Exercice. (TD3 Ex9) Montrer que $a^{m+10n} \equiv a^m \pmod{11}$ pour tout $a \in \mathbb{Z}$ et $m, n \geq 1$. Déterminer $2019^{9102} \bmod 11$.

Solution. $m + 10\, n \equiv m \pmod{10} \Longrightarrow a^{m+10n} \equiv a^m \pmod{11}$. Alors $2019 \equiv 2 \times (-1)^3 + 1 \times (-1) + 9 \equiv 6 \equiv -5 \pmod{11}$, donc $2019^{9102} \equiv (-5)^2 \equiv 25 \equiv 3 \pmod{11}$

Exercice. (TD3 Ex14) Pour $n \in \mathbb{N}$, on note $a_n = 3^n$, $b_n = 4^n$ et $c_n = 1018 \times 2018^n + 1026 \times 2019^n$. Calculer $a_n \bmod 13$, $b_n \bmod 13$ et $c_n \bmod 13$.

Solution. Tout d'abord, $13 \nmid 3$ et $13 \nmid 4$. $1001 = 7 \times 11 \times 13 \equiv 0 \pmod{13}$, donc $2018 \equiv 3 \pmod{13}$ et $2019 \equiv 4 \pmod{13}$. Alors $c_n \equiv 4 \times 3^n - 4^n \equiv 4\, a_n - b_n \pmod{13}$. Pour tout $n \in \mathbb{N}$, on prend n_0 est le reste de $n \bmod 12$. Alors $a_n \equiv 3^{n_0} \pmod{13}$ et $b_n \equiv 4^{n_0} \pmod{13}$.

n	0	1	2	3	4	5	6
$3^n \bmod 13$	1	3	-4	1	3	-4	1
$4^n \bmod 13$	1	4	3	-1	-4	-3	1
$c_n \bmod 13$ en utilisant $c_n \equiv 4\, a_n - b_n \pmod{13}$	3	-5	-6	5	3	0	3

Donc les ordres de $3 \pmod{13}$ et $4 \pmod{13} \in (\mathbb{Z}/13\,\mathbb{Z})^\times$ sont respectivement 3 et 6. Les valeurs de a_n, b_n, c_n modulo 13 ne dépend que de $n \bmod 6$.

Cas particulier $n = p^r$. $a^m \bmod p^r$ pour $m \geq 1$

Cas $\gcd(a, n) = 1$, c'est-à-dire, $p \nmid a$.

1. On a $a^{\varphi(n)} \equiv 1 \pmod n$. On calcule le reste $m \equiv m_0 \pmod{\varphi(n)}$. Alors $a^m \equiv a^{m_0} (a^{\varphi(n)})^{(m-m_0)/\varphi(n)} \equiv a^{m_0} \pmod n$.
2. Évaluer $a^{m_0} \bmod n$ (on peut remplacer a par le reste $a \bmod n$).

Cas $p \mid a$. On écrit $a = p^{v_p(a)}\, a_0$, alors $p^{m v_p(a)} \mid a^m$. Si $r \leq m\, v_p(a)$, alors le reste est 0. Sinon, il suffit de déterminer $a_0^m \bmod p^{r - m v_p(a)}$ où $p \nmid a_0$.

Exemple. Pour évaluer $12^{10} \bmod 3^{100}$, on écrit $12 = 3^1 \times 4$, alors $12^{10} = 3^{10} \times 4^{10}$. Pour évaluer $3^{10} \times 4^{10} \bmod 3^{100}$, il suffit d'évaluer $4^{10} \bmod 3^{90}$ (parce que si $4^{10} \equiv b \pmod{3^{90}}$, alors $3^{10} \times 4^{10} \equiv 3^{10}\, b \pmod{3^{90} \times 3^{10} = 3^{100}}$).

8 Séance 25 nov 2020

Exercice. (TD3 Ex5(2), pas bon) Déterminer $3^{15} \bmod 5^3$.

Solution. $\varphi(5^3)=100$. $15=1+2+2^2+2^3$ donc $3^{15}=3^1\,3^2\,3^4\,3^8$, donc il suffit d'évaluer (on note que $3^{2^n}=(3^{2^{n-1}})^2$)

n	0	1	2	3
$3^{2^n} \bmod 5^3$	3	9	-44	$44^2 \bmod 5^3$

Cas particulier $n=2^r, r\geq 3$.

Cas $2\nmid a$. On a $a^{\varphi(n)/2}\equiv 1 \pmod{2^r}$ où $\varphi(n)/2=2^{r-2}$. Donc évaluer $a^m \bmod n$:

1. Évaluer $m \bmod \varphi(n)/2 =: m_0$.
2. Évaluer $a^{m_0} \bmod n$, c'est le résultat de $a^m \bmod n$.

Question. (TD3 Ex11.1) Montrer que $2\nmid a \Longrightarrow a^2\equiv 1 \pmod 8$ (En effet, ici $r=3$)

Question. (TD3 Ex5(1)) Déterminer $3^{15} \bmod 2^3$. $3^{15}=(3^2)^7\,3\equiv 3 \pmod 8$

Cas $2\mid a$.

Cas général. 1 étape: factoriser $n=p_1^{r_1}\cdots p_s^{r_s}$.

Cas général. (Important)

1. Évaluer $a^m \bmod p_j^{r_j} =: \alpha_j$ pour $j=1,2,\ldots,s$ par les méthodes au-dessus.
2. Résoudre le système d'équations $(x\equiv \alpha_j \pmod{p_j^{r_j}})_{j=1}^s$.

Cas $\gcd(a,n)=1$. On peut utiliser l'amélioration de théorème d'Euler: $a^{\operatorname{ppcm}(\varphi(p_1^{r_1}),\ldots,\varphi(p_s^{r_s}))}\equiv 1 \pmod n$ (si $p_j^{r_j}=2^{r_j}$, on peut remplacer $\varphi(p_j^{r_j})$ par $\varphi(p_j^{r_j})/2$). En effet, ce nombre est « optimal ». Alors on peut calculer $m \bmod \operatorname{ppcm}(\varphi(p_1^{r_1}),\ldots,\varphi(p_s^{r_s})) =: m_0$, alors on calcule $a^{m_0} \bmod n$.

Question. (TD3 Ex10) Déterminer $2019^{2018} \bmod 91$.

Solution. $91=7\times 13$. $2019\equiv 17 \pmod{91}$ ($7\times 13 \mid 1001=7\times 11\times 13$), donc $2019^{2018}\equiv 17^{2018} \pmod{91}$. $\gcd(17, 91)=1$. On peut utiliser deux méthodes pour évaluer $17^{2018} \pmod{91}$:

1. On peut évaluer $\operatorname{ppcm}(\varphi(7),\varphi(13))=\operatorname{ppcm}(6,12)=12$, donc $17^{12}\equiv 1 \pmod{91}$ par l'amélioration du théorème d'Euler. On éavlue $2018 \bmod 12$. $2018/12=1009/6\in\mathbb{Z}+1/6\Rightarrow 2018 \bmod 12=2\Rightarrow 17^{2018}\equiv 17^2\equiv 289-91\times 2\equiv 16 \pmod{91}$.
2. Alternativement, on peut évaluer $17^{2018} \bmod 7=2$ et $17^{2018} \bmod 13=3$. Alors il suffit de résoudre le système $(x\equiv 2 \pmod 7, x\equiv 3 \pmod{13})\Rightarrow (x\equiv 16 \pmod{91})$

Exercice. (TD3 Ex16) Montrer que pour tout $n\in\mathbb{N}_{>0}$, on a $19 \mid 2^{2^{6n+2}}+3$.

Solution. On commence par déterminer $2^{6n+2} \bmod 18$. $18=2\times 3^2$ et $\gcd(2,18)=2\neq 1$. Pour cela, il faut déterminer $2^{6n+2} \bmod 2$ et $2^{6n+2} \bmod 3^2$. Tout d'abord, $2^{6n+2}\equiv 0 \pmod 2$. Ensuite, $\varphi(3^2)=2\times 3=6$, et $6n+2\equiv 2 \pmod{3^2}$, alors $2^{6n+2}\equiv 2^2 \pmod{3^2}$. Il reste de résoudre le système $(x\equiv 0 \pmod 2, x\equiv 4 \pmod 9)$. La solution est $x\equiv 4 \pmod{18}$. Alors $2^{2^{6n+2}}\equiv 2^4\equiv -3 \pmod{19}\Longrightarrow 19 \mid 2^{2^{6n+2}}+3$.

9 Séance 30 nov 2020

Exercice. (TD3 Ex11.2,3) Soit $a \in \mathbb{Z}$.

1. Montrer que $\operatorname{pgcd}(a,6)=1 \Longrightarrow a^2 \equiv 1 \pmod{24}$.
2. Montrer que $a^{13} \equiv a \pmod{2730}$.

Solution.

1. $24 = 2^3 \times 3$. Alors il suffit ($\operatorname{pgcd}(2^3,3)=1$) de montrer que $a^2 \equiv 1 \pmod{2^3}$ et $a^2 \equiv 1 \pmod{3}$. D'autant que $\operatorname{pgcd}(2, a)=1$, on a $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ pour $n \geq 3$ ($\varphi(2^n)/2 = 2^{n-2}$). En particulier, $a^2 \equiv 1 \pmod{2^3}$. D'autant que $3 \nmid a \Longrightarrow a^2 \equiv 1 \pmod{3}$.
2. $2730 = 2 \times 3 \times 5 \times 7 \times 13$, alors il suffit de montrer que $a^{13} \equiv a \pmod{2,3,5,7,13}$. Par exemple, pour le premier 7, on a $a^7 \equiv a \pmod{7}$, alors $a^{6k+1} \equiv a \pmod{7}$ où $k \in \mathbb{N}$ (soit par récurrence, soit la méthode suivante: quand $7 \nmid a$, alors par le petit théorème de Fermat, $a^6 \equiv 1$ alors $a^{6k+1} \equiv (a^6)^k\, a \equiv a \pmod{7}$; quand $7 \mid a$, alors $7 \mid a$ et $7 \mid a^{6k+1}$, donc $a \equiv 0 \equiv a^{6k+1} \pmod{7}$.

Exercice. (TD4 Ex3.3) Montrer que $n \equiv 1 \pmod{12} \Longrightarrow a^n \equiv a \pmod{91}$.

Problème. Énumerer toutes les valeurs possibles de $a^m \bmod n$.

1. Factoriser $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
2. Énumerer toutes les valeurs possible de $a^m \bmod p_i^{\alpha_i}$ (ici, on utilise l'améloration de théorème d'Euler pour simplifier le calcul).
3. Résoudre des systèmes d'équations $x \equiv \beta_i \pmod{p_i^{\alpha_i}}$.

Exercice. (TD4 Ex3.1, Ex3.2) Déterminer les valeurs possibles de $a^{12} \bmod 7$, de $a^{12} \bmod 13$ et de $a^{12} \bmod 91$ pour $a \in \mathbb{Z}$. Idem pour a^6 au lieu de a^{12}.

Solution.

1. Déterminer toutes les valeurs possibles de $a^{12} \bmod 91$:
   a. $91 = 7 \times 13$
   b. $a^{12} \bmod 7$: si $7 \mid a$, alors $a^{12} \equiv 0 \pmod{7}$. Sinon, par le théorème de Fermat, on a $a^6 \equiv 1 \pmod{7}$, donc $a^{12} \equiv 1 \pmod{7}$. En résumé, $a^{12} \equiv 0, 1 \pmod{7}$. Parallèllement, $a^{12} \equiv 0, 1 \pmod{13}$.
   c. Pour déterminer toutes les valeurs possibles de $a^{12} \bmod 7 \times 13$, il suffit de résoudre les systèmes

$$\begin{cases} x \equiv \alpha \pmod{7} \\ x \equiv \beta \pmod{13} \end{cases}$$

   pour tout $\alpha \in \{0,1\}$ et $\beta \in \{0,1\}$. $2 \times 7 - 13 = 1$, on a $x \equiv -13\,\alpha + 14\,\beta \pmod{7 \times 13}$, donc toutes les valeurs possibles de $a^{12} \bmod 7 \times 13$ sont $0, 14, -13, 1$.
2. Déterminer toutes les valeurs possibles de $a^6 \bmod 91$:
   a. $91 = 7 \times 13$
   b. Indication: pour déterminer toutes les valeurs possibles de $a^6 \bmod 13$, il faut énumérer $a \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6$. $a^6 = (a^2)^3$

   Quand $7 \mid a$, on a $a^6 \equiv 0 \pmod{7}$. Quand $7 \nmid a$, alors $a^6 \equiv 1 \pmod{7}$ par le théorème de Fermat. Donc $a^6 \equiv 0, 1 \pmod{7}$.

   Pour $a^6 \bmod 13$: $a^2 \equiv 0, 1, 4, -4, 3, -1, -3 \equiv 0, \pm 1, \pm 3, \pm 4 \pmod{13}$, donc ($(-b)^3 = -b^3$, donc $(\pm b)^3 = \pm b^3$) $a^6 = (a^2)^3 \equiv 0, \pm 1 \pmod{13}$. Donc il reste de résoudre

$$\begin{cases} x \equiv \alpha \pmod{7} \\ x \equiv \beta \pmod{13} \end{cases}$$

pour $\alpha \in \{0,1\}$ et $\beta \in \{0,\pm 1\}$. $x \equiv -13\,\alpha + 14\,\beta \pmod{7\times 13}$, donc les valeurs possibles de $a^6 \bmod 7\times 13$ sont

Exercice. (TD3 Ex12) Soit $x \in \mathbb{Z}$. Montrer que

1. si $\operatorname{pgcd}(x,30)=1$, alors on a $x^4 \equiv 1 \pmod{240}$.
2. $x^4 \equiv 0 \text{ ou } 1 \pmod q$ où $q = 2^4, 3, 5$.
3. $x^4 \equiv x^8 \pmod{240}$
4. Pour tout $n \geq 0$, $x^{n+4} \equiv x^{n+8} \pmod{240}$
5. $x^4 \equiv 0, 16, 96, 160 \pmod{240}$ ou $x^4 \equiv 1, 81, 145, 225 \pmod{240}$.

Solution.

1. $240 = 2^4 \times 3 \times 5$. Alors par l'amélioration de théorème d'Euler, quand $\operatorname{pgcd}(x, 30 = 2\times 3\times 5) = 1$, alors $x^4 \equiv x^{2^4-2} \equiv 1 \pmod{2^4}$, $x^2 \equiv 1 \pmod 3$, $x^4 \equiv 1 \pmod 5$. Donc $x^4 \equiv 1 \pmod{\operatorname{ppcm}(2^4,3,5) = 240}$.
2. $q = 2^4$: si $2 \mid x$ alors $2^4 \mid x^4 \Rightarrow x^4 \equiv 0 \pmod{2^4}$. Si $2 \nmid x$, alors $x^4 \equiv 1 \pmod{2^4}$ (voir au-dessus).

   $q = 3, 5$: si $3 \mid x$, alors ... . Si $3 \nmid x$, alors ....
3. D'autant que $0^2 = 0$ et $1^2 = 1$, alors $(x^4)^2 \equiv x^4 \pmod q$ où $q = 2^4, 3, 5$, alors $x^8 \equiv x^4 \pmod{\operatorname{ppcm}(2^4,3,5) = 240}$.
4. $x^{n+4} \equiv x^n\, x^4 \equiv x^n\, x^8 \equiv x^{n+8} \pmod{240}$
5. Il reste de résoudre les systèmes

$$\begin{cases} x \equiv \alpha \pmod{2^4} \\ x \equiv \beta \pmod 3 \\ x \equiv \gamma \pmod 5 \end{cases}$$

   pour $\alpha, \beta, \gamma \in \{0,1\}$. Truc: $2^4 = 3\times 5 + 1$. Donc cela va mieux de commencer par résoudre

$$\begin{cases} x \equiv \beta \pmod 3 \\ x \equiv \gamma \pmod 5 \end{cases}$$

   D'autant que $2\times 3 - 5 = 1$, alors la solution est $x \equiv -5\,\beta + 6\,\gamma \pmod{15}$. Il reste de résoudre

$$\begin{cases} x \equiv \alpha \pmod{16} \\ x \equiv 6\,\beta - 5\,\gamma \pmod{15} \end{cases}$$

   Solution: $x \equiv -15\,\alpha + 16\,(6\,\beta - 5\,\gamma) \pmod{15\times 16}$. On prend $\alpha, \beta, \gamma \in \{0,1\}$.

10 Séance 2 déc 2020

Définition. *Soit* $n \in \mathbb{N}_{>0}$. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ *(i.e.* $\gcd(a,n)=1$*) est un* générateur *si l'ordre de* a *est* $\varphi(n)$ *(Rappelons que* $\mathrm{ord}(a) \mid \varphi(n)$*).*

Exercice. (TD4 Ex5) Soit $a \in \mathbb{Z}$.

1. Si $17 \nmid a$, alors $a \pmod{17}$ générateur ssi $a^8 \not\equiv 1 \pmod{17}$. Trouver un tel générateur.
2. Si $3 \nmid a$, alors $a \pmod{27}$ générateur ssi $a^6, a^9 \not\equiv 1 \pmod{27}$. Trouver un tel générateur.

Solution.

1. $\mathrm{ord}(a) \mid \varphi(17) = 16 = 2^4$, alors $\mathrm{ord}(a) = 16$ ssi $\mathrm{ord}(a) \nmid 8$ ssi $a^8 \not\equiv 1 \pmod{17}$ (en général, pour $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $a^m \equiv 1 \pmod{n}$ ssi $\mathrm{ord}(a) \mid m$).

   Pour trouver un tel générateur, $a = 1, 2, \ldots$. Tout d'abord, 1 n'est pas un générateur. $2^8 = (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$ donc 2 n'est pas un générateur (en effet, $\mathrm{ord}(2) = 8$). On évalue $3^8 \bmod 17$: $3^2 \equiv -8 \pmod{17}$, $3^4 = (3^2)^2 \equiv -4 \pmod{17}$, $3^8 \equiv -1 \not\equiv 1 \pmod{17}$, donc 3 est un générateur.

2. $\varphi(27) = 18$. Donc $\mathrm{ord}(a) \mid 18 = 2 \times 3^2$, $\mathrm{ord}(a) = 18$ ssi $\mathrm{ord}(a) \nmid 6$ et $\mathrm{ord}(a) \nmid 9$ ssi $a^6 \not\equiv 1 (\mathrm{mod}\, 27)$ et $a^9 \not\equiv 1 (\mathrm{mod}\, 27)$. Donc on teste $a = 1, 2, \ldots$ $2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 64 \not\equiv 1 (\mathrm{mod}\, 27)$ et $2^9 \equiv (2^3)^3 \equiv 8^3 \equiv (-1)^3 \equiv -1 \not\equiv 1 (\mathrm{mod}\, 9) \Rightarrow 2^9 \not\equiv 1 (\mathrm{mod}\, 27)$. Donc 2 est un générateur.

   Remarque. En général, soit $m, n \in \mathbb{N}$, $m \mid n$. Alors $m = n$ ssi $n/m = 1$ ssi pour tout premier $p \mid n$, on a $m \nmid (n/p)$.

Exercice. (TD4 Ex2) Soient $a, b \in \mathbb{Z}$. Montrer que

1. si $2 \nmid a$ et $5 \nmid a$, alors $a^{100} \equiv 1 \pmod{1000}$.
2. $b^{100} \equiv 0, 1, 376, 625 \pmod{1000}$.

Solution.

1. $1000 = 2^3 \times 5^3$, alors quand $2 \nmid a$ et $5 \nmid a$, on a $a^2 \equiv 1 \pmod{2^3}$ et $a^{100} \equiv a^{\varphi(5^3)} \equiv 1 \pmod{5^3}$. Donc $a^{100} \equiv 1 \pmod{1000 = \mathrm{ppcm}(2^3, 5^3)}$.
2. Si $2 \mid b$ alors $2^3 \mid b^{100}$, sinon $b^{100} \equiv (b^2)^{50} \equiv 1 \pmod{2^3}$. Si $5 \mid b$, alors $5^3 \mid b^{100}$, sinon $b^{100} \equiv 1 \pmod{5^3}$ par thm d'Euler. Conclusion: $b^{100} \equiv 0, 1 (\mathrm{mod}\, 2^3)$ et $b^{100} \equiv 0, 1 (\mathrm{mod}\, 5^3)$. Il suffit de résoudre le système $x \equiv \alpha (\mathrm{mod}\, 2^3)$ et $x \equiv \beta \pmod{5^3}$. On a $125 = 15 \times 8 + 5$, $8 = 1 \times 5 + 3$, $5 = 1 \times 3 + 2$, $3 = 1 \times 2 + 1$. Alors $5 = 125 - 15 \times 8$, $3 = 8 - 1 \times 5 = 8 - 1 \times (125 - 15 \times 8) = 16 \times 8 - 125$, $2 = 5 - 1 \times 3 = (125 - 15 \times 8) - (16 \times 8 - 125) = 2 \times 125 - 31 \times 8$, $1 = 3 - 1 \times 2 = (16 \times 8 - 125) - 1 \times (2 \times 125 - 31 \times 8) = 47 \times 8 - 3 \times 125$. Alors $x \equiv -3 \times 125\,\alpha + 47 \times 8\,\beta \pmod{1000}$. On prend $\alpha \in \{0, 1\}$, $\beta \in \{0, 1\}$, on en déduit le résultat.

Problème. (Si le temps le permet) Résoudre une équation $f(x) \equiv 0 \pmod{n}$ où $f \in \mathbb{Z}[x]$ se factorise comme $a(x - r_1) \cdots (x - r_m)$ où $a, r_1, \ldots, r_m \in \mathbb{Z}$.

On explique par exemples:

Exercice. (TD4 Ex6) Étude de l'équation $x^2 \equiv 1 \pmod{n}$.

1. Montrer que si $n = p$ (premier), alors les solutions sont $\pm 1 \pmod{n}$.
2. Montrer que si $n = p^r$ ($p > 2$ premier, $r \in \mathbb{N}_{>0}$), alors les solutions sont $\pm 1 \pmod{n}$.
3. Combien y a-t-il de solutions quand $n = 91$ ou $n = 105$?
4. Montrer que si $n = 2^r$ ($r > 2$), alors les solutions sont $\pm 1, \pm(1 + n/2) \pmod{n}$.

Solution.

1. $x^2 \equiv 1 (\mathrm{mod}\, p)$ ssi $p \mid (x-1)(x+1)$ ssi (p est premier) $p \mid x - 1$ ou $p \mid x + 1$ ssi $x \equiv \pm 1 \pmod{p}$.

2. $x^2 \equiv 1 (\mathrm{mod}\, p^r)$ ssi $p^r \mid (x-1)(x+1)$. En particulier, $p \mid x-1$ ou $p \mid x+1$. Si $p \mid x-1$, alors $x+1 \equiv 2 \not\equiv 0 (\mathrm{mod}\, p) \Rightarrow p \nmid x+1 \Rightarrow \mathrm{pgcd}(p^r, x+1) = 1 \xRightarrow{p^r \mid (x-1)(x+1)} p^r \mid x-1$. Parallèllement, si $p \mid x+1$ alors on a $p^r \mid x+1$. Conclusions: si $p^r \mid (x-1)(x+1)$, alors $x \equiv \pm 1 \ (\mathrm{mod}\, p^r)$. Vérifier que ce sont les solutions.

3. On factorise $91 = 7 \times 13$ et $105 = 3 \times 5 \times 7$. Alors $x^2 \equiv 1 (\mathrm{mod}\, 91)$ ssi $x^2 \equiv 1 (\mathrm{mod}\, 7)$ et $x^2 \equiv 1 (\mathrm{mod}\, 13)$ ssi $x \equiv \pm 1 (\mathrm{mod}\, 7)$ et $x \equiv \pm 1 (\mathrm{mod}\, 13)$. Par le thm de reste chinois, il y a $2 \times 2 = 4$ solutions quand $n = 91$. Parallèllement, pour $n = 3 \times 5 \times 7$, il y a $2 \times 2 \times 2 = 8$ solutions.

4. $2^r \mid (x-1)(x+1) \Rightarrow 2 \mid x-1$. Donc $2^{r-2} \mid \frac{x+1}{2} \frac{x-1}{2} \Rightarrow 2 \mid \frac{x+1}{2}$ ou $2 \mid \frac{x-1}{2}$. Si $2 \mid \frac{x-1}{2}$, alors $\frac{x+1}{2} = \frac{x-1}{2} + 1 \equiv 1 (\mathrm{mod}\, 2) \Rightarrow \mathrm{pgcd}\big(2^{r-2}, \frac{x+1}{2}\big) = 1 \xRightarrow{2^{r-2} \mid \frac{x+1}{2} \frac{x-1}{2}} 2^{r-2} \mid \frac{x-1}{2} \Rightarrow 2^{r-1} \mid x-1$. Si $2 \mid \frac{x+1}{2}$, parallèllement, on a $2^{r-1} \mid x+1$. Conclusion: $x \equiv \pm 1 \ (\mathrm{mod}\, 2^{r-1} = n/2)$. On peut vérfier que quand $x \equiv \pm 1 (\mathrm{mod}\, 2^{r-1})$, on a $x^2 \equiv 1 \ (\mathrm{mod}\, n)$.

Exercices non-traités

Exercice. (TD4 Ex7) Étude de l'équation $x^2 \equiv x \pmod{n}$.

1. Montrer que si $n = p^r$ (p premier), alors les solutions sont $x \equiv 0, 1 \pmod{n}$.
2. Combien y a-t-il de solutions quand $n = 10, 100, 1000, 840$?

Exercice. (TD3 Ex15, pas important) Soient $x, y, z \in \mathbb{Z}$. Montrer que

1. $x^2 \equiv 0, 1, 4 \pmod{8}$
2. Si $4 \mid (x^2 + y^2 + z^2)$, alors $2 \mid x$ et y et z.
3. Si $x^2 + y^2 + z^2 \equiv 3 \pmod{4}$, alors $2 \nmid x$ ou y ou z, et $x^2 + y^2 + z^2 \equiv 3 \pmod{8}$.
4. $x^2 + y^2 + z^2 \neq 4^k (8l + 7)$, $k, l \in \mathbb{N}$.

11 Séance 7 déc 2020

Perdu. Voir l'ancien PDF.

12 Séance 9 déc 2020

Perdu. Voir l'ancien PDF.

13 Séance 14 déc 2020

Exercice. (CC6 Q1) Soit p un premier. Montrer que $(\mathbb{Z}[1/p]\setminus\{0\},\cdot)$ n'est pas un groupe.

Solution. On note que $\mathbb{Z}[1/p]\setminus\{0\}\subseteq\mathbb{Q}\setminus\{0\}$ et $(\mathbb{Q}\setminus\{0\},\cdot)$ est un groupe. Donc si $(\mathbb{Z}[1/p]\setminus\{0\},\cdot)$ est un groupe, alors il est un sous-groupe de $(\mathbb{Q}\setminus\{0\},\cdot)$. On va trouver un élément $x\in\mathbb{Z}[1/p]\setminus\{0\}$ t.q. $x^{-1}\notin\mathbb{Z}[1/p]\setminus\{0\}$.

(Il faut chercher soigneusement x. Par exemple, si $x=p$, alors $x^{-1}=p^{-1}\cdot 1\in\mathbb{Z}[1/p]\setminus\{0\}$. En général, si $x=p^n$ où $n\in\mathbb{N}_{>0}$, alors $x^{-1}=p^{-n}\cdot 1\in\mathbb{Z}[1/p]\setminus\{0\}$)

On prend un premier $q\neq p$. On va monter que $q^{-1}\notin\mathbb{Z}[1/p]\setminus\{0\}$. En effet, pour tout $p^{-m}n\in\mathbb{Z}[1/p]$, on a $v_q(p^{-m}n)=v_q(n)\geq 0$ mais $v_q(q^{-1})=-1<0$. Donc $q^{-1}\in\mathbb{Z}[1/p]\setminus\{0\}$.

Problème. Étant donné un premier p concret, montrer que $(\mathbb{Z}/p\,\mathbb{Z})^\times$ est cyclique et trouver un générateur.

Remarque. À ce stade, il faut toujours trouver un générateur (rappel: TD4 Ex5).

Exercice. (TD5 Ex7.5) $(\mathbb{Z}/4\,\mathbb{Z},+)\cong((\mathbb{Z}/5\,\mathbb{Z})^\times,\cdot)$.

Solution. Il faut trouver un générateur de $(\mathbb{Z}/5\,\mathbb{Z})^\times$. Il faut tester si $2\pmod 5$ est un générateur. $\varphi(5)=4$ alors que $2^{4/2}\not\equiv 1\pmod 5$, donc 2 est un génerateur (parce que $\mathrm{ord}_{(\mathbb{Z}/5\mathbb{Z})^\times}(2)\mid\varphi(5)$), donc $(\mathbb{Z}/5\,\mathbb{Z})^\times$ est un groupe cyclique et l'appli $\mathbb{Z}/4\,\mathbb{Z}\to(\mathbb{Z}/5\,\mathbb{Z})^\times, n\pmod 4\mapsto 2^n$ est isomorphisme.

Exercice. (TD5 Ex4) Soit $(G,*)$ un groupe. Décrire tous les morphismes de groupes $\mathbb{Z}\to(G,*)$.

Solution. En effet, on a une bijection d'ensembles $\{\text{morphismes de groupes } \mathbb{Z}\to(G,*)\}\xrightarrow{\sim}G$ donné par $f\mapsto f(1)$ dont l'inverse est donné par $G\to\{\text{morphismes de groupes } \mathbb{Z}\to(G,*)\}, g\mapsto(\mathbb{Z}\to(G,*), n\mapsto g^n)$.

Remarque. On prend la valeur de f en 1, parce que 1 est un générateur de $\mathbb{Z}$ (-1 aussi), $f(n)=f(1)^n$ pour tout $n\in\mathbb{Z}$.

Exercice. (TD5 Ex12) Soit $g\in G$ d'ordre fini et soit $f:G\to H$ un morph de groupes. Montrer que l'ordre de $f(g)$ divise l'ordre de g. Si f est injectif, montrer que l'ordre de $f(g)$ est égal à l'ordre de g.

Solution. $f(g)^{\mathrm{ord}_G(g)}=f(g^{\mathrm{ord}_G(g)})=f(e_G)=e_H$, donc $\mathrm{ord}_H(f(g))\mid\mathrm{ord}_G(g)$ (Rappelons que $g^n=e$ ssi $\mathrm{ord}(g)\mid n$).

En suite, si f est injectif, alors $\mathrm{Ker}(f)=\{e_G\}$. Alors pour tout $n\in\mathbb{Z}$, si $f(g)^n=e_H$, alors $f(g^n)=f(g)^n=e_H\Longrightarrow g^n=e_G\Longrightarrow\mathrm{ord}_G(g)\mid n$. En particulier, $\mathrm{ord}_G(g)\mid\mathrm{ord}_H(f(g))$. Alors $\mathrm{ord}_H(f(g))=\mathrm{ord}_G(g)$.

Remarque. Soit $g\in G$ avec $\mathrm{ord}_G(g)<\infty$. Le morphisme $\mathbb{Z}\to G, n\mapsto g^n$ de groupes induit un morphe injectif $\mathbb{Z}/\mathrm{ord}_G(g)\hookrightarrow G$ de groupes. En particulier, $\mathrm{ord}_G(g^k)=\mathrm{ord}_G(g)/\mathrm{pgcd}(|k|,m)$. Ici, il s'agit de calculer $\mathrm{ord}_G(g^k)$ à partir de $\mathrm{ord}_G(g)$.

Exercice. (TD5 Ex5) Montrer: une app $f:\mathbb{Z}\to\mathbb{Z}$ est un morphisme de groupes ss'il existe $a\in\mathbb{Z}$ t.q. $f(x)=a\,x$ pour tout $x\in\mathbb{Z}$. Déterminer le noyau et l'image de f. Quand est-ce que f est un isomorphisme de groupes?

Solution. Tout d'abord, si $f(x)=a\,x$ pour tout $x\in\mathbb{Z}$, alors f est un morphisme de groupes. En revanche, si $f:\mathbb{Z}\to\mathbb{Z}$ est un morphisme de groupe, alors $f(x)=x\,f(1)$. On prend $a=f(1)$. Quand $f(x)=a\,x$, $\mathrm{Ker}(f)=\{x\in\mathbb{Z}\mid a\,x=0\}$.

Cas $a=0$. $\mathrm{Ker}(f)=\mathbb{Z}$ et $\mathrm{Im}(f)=0$.

Cas $a\neq 0$. $\mathrm{Ker}(f)=0$ et $\mathrm{Im}(f)=a\,\mathbb{Z}$.

f est un isomorphisme ssi $\mathrm{Ker}(f)=0$ et $\mathrm{Im}(f)=\mathbb{Z}$, donc $a\neq 0$ et $a\,\mathbb{Z}=\mathbb{Z}$, donc $1\in a\,\mathbb{Z}\Longrightarrow a\mid 1\Longrightarrow a=\pm 1$. En revanche, si $a=\pm 1$, alors $a\,\mathbb{Z}=\mathbb{Z}$ et f est un isomorphisme.

Exercice. (TD5 Ex11) L'appli f est-elle un morphisme de groupes? Si c'est le cas, déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

1. $\boldsymbol{f:(\mathbb{C}\setminus\{0\},\cdot)\to(\mathbb{R}\setminus\{0\},\cdot),z\mapsto|z|.}$
2. $f:(\mathbb{Z}^2,+)\to(\mathbb{Z},+),(a,b)\mapsto a-b.$
3. $f:(\mathbb{Z}^2,+)\to(\mathbb{Z}/2\,\mathbb{Z},+),(a,b)\mapsto a-b\,(\mathrm{mod}\,2).$
4. $f_4:(\mathbb{Z}^2,+)\to(\mathbb{Z},+)\times(\mathbb{Z}/2\,\mathbb{Z},+),(a,b)\mapsto(a-b,b\,(\mathrm{mod}\,2)).$
5. $\boldsymbol{f:(\mathbb{Z}^3,+)\to(\mathbb{Q}_{>0},\cdot),(a,b,c)\mapsto 2^a\,3^b\,5^c.}$
6. $\boldsymbol{f:(\mathbb{Z}^3,+)\to(\mathbb{Q}_{>0},\cdot),(a,b,c)\mapsto 2^a\,3^b\,6^c.}$

Solution.

1. Oui. $\mathrm{Ker}(f)=\{z\in\mathbb{C}\,|\,|z|=1\}$. $\mathrm{Im}(f)=\mathbb{R}_{>0}$ parce que, tout d'abord, $\mathrm{Im}(f)=\{|z|\,|\,z\in\mathbb{C}\setminus\{0\}\}\subseteq\mathbb{R}_{>0}$. En revanche, pour tout $r\in\mathbb{R}_{>0}$, on a $|r|=r$ où $r\in\mathbb{C}\setminus\{0\}$. Donc $\mathbb{R}_{>0}\subseteq\mathrm{Im}(f)$. En conclusion, $\mathrm{Im}(f)=\mathbb{R}_{>0}$.

5. Oui. Tout d'abord, les deux sont des groupes. En suite, $f(a+a',b+b',c+c')=2^{a+a'}\,3^{b+b'}\,5^{c+c'}=2^a\,2^{a'}\,3^b\,3^{b'}\,5^c\,5^{c'}=2^a\,3^b\,5^c\,2^{a'}\,3^{b'}\,5^{c'}=f(a,b,c)+f(a',b',c')$. Ensuite, $\mathrm{Ker}(f)=\{(a,b,c)\mid 2^a\,3^b\,5^c=1\}$. Alors $v_2(2^a\,3^b\,5^c)=v_2(1)=0\Longrightarrow a=0$. Parallèllement, on prend v_3 et v_5, on a $b=c=0$. Donc $\mathrm{Ker}(f)=\{(0,0,0)\}$ (f est injectif). $\mathrm{Im}(f)=\{2^{\mathbb{Z}}\times 3^{\mathbb{Z}}\times 5^{\mathbb{Z}}\}$.

6. Oui. $\mathrm{Ker}(f)=\{(a,b,c)\mid 2^a\,3^b\,6^c=1\}$. On prend v_2 et v_3, $a+c=b+c=0$. Donc $\mathrm{Ker}(f)=\{(-c,-c,c)\mid c\in\mathbb{Z}\}$. $\mathrm{Im}(f)=\{2^{\mathbb{Z}}\times 3^{\mathbb{Z}}\}$ ($f(a,b,c)=f(a+c,b+c,0)$).

Exercice. (TD5 Ex15) Notons G le groupe $((\mathbb{Z}/16\,\mathbb{Z})^\times,\cdot)$ des éléments inversibles de $\mathbb{Z}/16\,\mathbb{Z}$.

1. Quel est l'ordre de G?
2. Énumérer les éléments de G et déterminer leurs ordres respectifs.
3. Le groupe G est-il cyclique?
4. Montrer que l'appli $f:\mathbb{Z}/2\,\mathbb{Z}\times\mathbb{Z}/4\,\mathbb{Z}\to(\mathbb{Z}/16\,\mathbb{Z})^\times,(a\,(\mathrm{mod}\,2),b\,(\mathrm{mod}\,4))\mapsto(-1)^a\,5^b\,(\mathrm{mod}\,16)$ est **bien définie**. Que peut-on dire de f?

Solution.

1. $\#G=\varphi(16)=8$.
2. $a(\mathrm{mod}\,16)\in\mathbb{Z}/16\,\mathbb{Z}$ est inversible ssi $\mathrm{pgcd}(a,16)=1$ ssi $2\nmid a$. Alors $(\mathbb{Z}/16\,\mathbb{Z})^\times=\{\pm1,\pm3,\pm5,\pm7(\mathrm{mod}\,16)\}$ (Rappelons que $\mathrm{ord}(g)\mid\varphi(16)=8$, donc $\mathrm{ord}(g)=2^k$). $\mathrm{ord}(1)=1$

$g^{2^k}\,(\mathrm{mod}\,16)$	$g=-1$	$g=\pm3$	$g=\pm5$	$g=\pm7$
$k=0$	-1	±3	±5	±7
$k=1$	1	-7	-7	1
$k=2$		1	1	

   Donc $\mathrm{ord}(-1)=\mathrm{ord}(\pm7)=2^1=2$ et $\mathrm{ord}(\pm3)=\mathrm{ord}(\pm5)=2^2=4$.
3. $\#G=8$ mais pour tout $g\in(\mathbb{Z}/16\,\mathbb{Z})^\times$, $\mathrm{ord}(g)\leq 4$, donc ....
4. Pour montrer que l'appli en question est bien définie, il suffit de vérifier que $(-1)^a\,5^b\equiv(-1)^{a'}\,5^{b'}(\mathrm{mod}\,16)$ quand $a\equiv a'(\mathrm{mod}\,2)$ et $b\equiv b'(\mathrm{mod}\,4)$. On note $a-a'=2\,c$ et $b-b'=4\,d$ alors $(-1)^{a-a'}\,5^{b-b'}=(-1)^{2c}\,(5^4)^d\equiv1\,(\mathrm{mod}\,16)$. On calcule $\mathrm{Ker}(f)$: $(a(\mathrm{mod}\,2),b(\mathrm{mod}\,4))\in\mathrm{Ker}(f)$ ssi $(-1)^a\,5^b\equiv1\,(\mathrm{mod}\,16)$. Alors $5^{2b}\equiv1\,(\mathrm{mod}\,16)\Rightarrow4=\mathrm{ord}(5)\mid2\,b\Rightarrow b$ est pair. Si $b/2$ est impair, alors $(-1)^a\,5^b\equiv\pm7\not\equiv1\,(\mathrm{mod}\,16)$. Donc $b/2$ est pair, c'est-à-dire, $4\mid b$, alors $5^b\equiv1\,(\mathrm{mod}\,16)\Rightarrow(-1)^a\equiv1(\mathrm{mod}\,16)$ donc a est pair. En conclusion, on a $(-1)^a\,5^b\equiv1\,(\mathrm{mod}\,16)$ ssi $2\mid a$ et $4\mid b$. Donc $\mathrm{Ker}(f)=\{(0,0)\}$ c'est-à-dire, f est injectif. D'autant que f est une application d'ensembles finis et $\#(\mathbb{Z}/2\,\mathbb{Z}\times\mathbb{Z}/4\,\mathbb{Z})=8=\#((\mathbb{Z}/16\,\mathbb{Z})^\times)$. Donc f est un isomorphisme.

14 Séance 16 déc 2020

Remarque. Pour un groupe fini G, on a $g^{\#G} = e \Longleftrightarrow \mathrm{ord}_G(g) \,|\, \#G$ (le théorème de Lagrange). Alors $\mathrm{ord}_G(g) = \#G$ ssi pour tout premier $p \,|\, \#G$, on a $g^{(\#G)/p} \neq e$. Peut-être vous n'avez pas encore vu le théorème de Lagrange, mais vous avez vu le cas particulier: $G = (\mathbb{Z}/n\,\mathbb{Z})^*$ (une autre notation: $(\mathbb{Z}/n\,\mathbb{Z})^\times$, c'est le théorème d'Euler, parce que $\#(\mathbb{Z}/n\,\mathbb{Z})^\times = \varphi(n)$). Voir TD4 Ex5 pour une exemple.

Exercice. (TD5 Ex13) Soit $n \in \mathbb{N}_{>0}$. Montrer que $\mu_n = (\{z \in \mathbb{C} \,|\, z^n = 1\}, \cdot)$ est un groupe cyclique d'ordre n. Définir un isomorphisme de groupes explicite $(\mathbb{Z}/n\,\mathbb{Z}, +) \xrightarrow{\sim} \mu_n$. Pour tout diviseur positif $d \,|\, n$, montrer que $\mu_d \subseteq \mu_n$ est un sous-groupe de μ_d (cyclique d'ordre d). Y a-t-il d'autres sous-groupes?

Solution. $\mu_n = \{\mathrm{e}^{2\pi i k/n} \,|\, k = 0, \ldots, n-1\}$ et $\mathrm{ord}_{\mu_n}(\mathrm{e}^{2\pi i/n}) = n$ parce que pour tout $\ell = 1, \ldots, k-1$, on a $(\mathrm{e}^{2\pi i/n})^\ell = \mathrm{e}^{2\pi i \ell/n} \neq 1$ (si vous avez vu le théorème de Lagrange, vous pouvez juste vérifier tous les diviseurs positifs $\ell \,|\, n$, mais ici, cela ne simplifie rien). Alors le groupe μ_n est cyclique. Explicitement, $\mathbb{Z}/n\,\mathbb{Z} \to \mu_n$ est donné par $k \,(\mathrm{mod}\, n) \mapsto (\mathrm{e}^{2\pi i/n})^k$. Alors pour tout $d \,|\, n$, on a μ_d est aussi un groupe cyclique, et $\mu_d \subseteq \mu_n$, donc μ_d est un sous-groupe de μ_n.

Lemme. *Pour un groupe cyclique fini G, tous les sous-groupes $H \subseteq G$ sont cyclique.*

Démonstration. $G = \{e, g, g^2, \ldots, g^{\#G-1}\}$. Si $H = \{e\}$, alors H est cyclique. Sinon, il existe $m \in \{1, \ldots, \#G-1\}$ t.q. $g^m \in H$. On prend le minimum $m_0 \in \{1, \ldots, \#G-1\}$ t.q. $g^{m_0} = e$. Alors pour tout $g^k \in H$ pour $k \in \{0, \ldots, \#G-1\}$, on prend la division d'Euclide $k = m_0\, q + r$ où $q, r \in \mathbb{Z}, 0 \leq r < m_0$. Alors $g^r = g^{k - m_0 q} = (g^{m_0})^{-q}\, g^k = g^k \in H$. D'autant que m_0 est minime, on a $r = 0$, c'est-à-dire, $m_0 \,|\, k$. En résumé, on a $H \subseteq \langle g^{m_0} \rangle$. D'autant que $g^{m_0} \in H$, on a $\langle g^{m_0} \rangle \subseteq H$. Donc $H = \langle g^{m_0} \rangle$ est cyclique. □

En particulier, il n'y a pas d'autres sous-groupes que μ_d.

Exercice. (TD5 Ex8) Soit G un groupe. Montrer que pour tout $g \in G$, l'app $f : G \to G, h \mapsto g\, h\, g^{-1}$ est un auto. Déterminer f^{-1}.

Solution. Tout d'abord, on vérifier que f est un morphisme de groupes. Pour tout $h, h' \in G$, on a $f(h)\, f(h') = g\, h\, g^{-1}\, g\, h'\, g^{-1} = g\, h\, (g^{-1}\, g)\, h'\, g^{-1} = g\, h\, h'\, g^{-1} = f(h\, h')$. Pour montrer que f est un automorphisme, il suffit montrer que $\mathrm{Ker}(f) = \{e\}$ et $\mathrm{Im}(f) = G$. Donc pour tout $h \in G$, si $f(h) = e$, alors $g\, h\, g^{-1} = e$. Donc $g\, h = (g\, h\, g^{-1})\, g = e\, g = g$ et $h = g^{-1}\, (g\, h) = g^{-1}\, g = e$. Donc $\mathrm{Ker}(f) = \{e\}$. Pour tout $h' \in G$, on a $f(g^{-1}\, h'\, g) = g\, (g^{-1}\, h'\, g)\, g^{-1} = (g\, g^{-1})\, h'\, (g\, g^{-1}) = h'$, donc $\mathrm{Im}(f) = G$. En résumé, f est un isomorphisme. $f^{-1} : G \to G, h' \mapsto g^{-1}\, h'\, g$.

Exercice. (TD5 Ex6) Montrer: une appli $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ est un morphisme de groupes si existe $a, b, c, d \in \mathbb{Z}$ t.q. $f(x, y) = (a\, x + b\, y, c\, x + d\, y)$ pour tout $(x, y) \in \mathbb{Z}^2$.

Solution. Il s'agit de vérifier que $f : \mathbb{Z}^2 \to \mathbb{Z}^2, (x, y) \mapsto (a\, x + b\, y, c\, x + d\, y)$ est un morphisme de groupes.

Exercices non-traités

Exercice. (TD5 Ex6') Montrer: une appli $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ est un morphisme de groupes, alors il existe $a, b, c, d \in \mathbb{Z}$ t.q. $f(x, y) = (a\,x + b\,y, c\,x + d\,y)$ pour tout $(x, y) \in \mathbb{Z}^2$. Déterminer $\mathrm{Ker}(f)$.

Exercice. (TD5 Ex4', le temps) Soit $(G, *)$ un groupe. Décrire tous les morphismes de groupes $\mathbb{Z}^2 \to (G, *)$.

Exercice. (TD5 Ex9, le temps) Soit G un groupe t.q. $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Exercice. (TD5 Ex10, le temps) Soit G un groupe. Montrer que l'app $g \mapsto g^{-1}$ est un morph de groupes ssi G est abélien.

15 Séance 4 jan 2021

Rappel:

Exercice. (TD4 Ex5) Soit $a \in \mathbb{Z}$.

1. Si $17 \nmid a$, alors $a \pmod{17}$ générateur ssi $a^8 \not\equiv 1 \pmod{17}$. Trouver un tel générateur.
2. Si $3 \nmid a$, alors $a \pmod{27}$ générateur ssi $a^6, a^9 \not\equiv 1 \pmod{27}$. Trouver un tel générateur.

Solution.

1. $\operatorname{ord}(a) \mid \varphi(17) = 16 = 2^4$, alors $\operatorname{ord}(a) = 16$ ssi $\operatorname{ord}(a) \nmid 8$ ssi $a^8 \not\equiv 1 \pmod{17}$ (en général, pour $a \in (\mathbb{Z}/n\,\mathbb{Z})^\times$, $a^m \equiv 1 \pmod{n}$ ssi $\operatorname{ord}(a) \mid m$).

   Pour trouver un tel générateur, $a = 1, 2, \ldots$. Tout d'abord, 1 n'est pas un générateur. $2^8 = (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$ donc 2 n'est pas un générateur (en effet, $\operatorname{ord}(2) = 8$). On évalue $3^8 \bmod 17$: $3^2 \equiv -8 \pmod{17}$, $3^4 = (3^2)^2 \equiv -4 \pmod{17}$, $3^8 \equiv -1 \not\equiv 1 \pmod{17}$, donc 3 est un générateur.

2. $\varphi(27) = 18$. Donc $\operatorname{ord}(a) \mid 18 = 2 \times 3^2$, $\operatorname{ord}(a) = 18$ ssi $\operatorname{ord}(a) \nmid 6$ et $\operatorname{ord}(a) \nmid 9$ ssi $a^6 \not\equiv 1 (\operatorname{mod} 27)$ et $a^9 \not\equiv 1 (\operatorname{mod} 27)$. Donc on teste $a = 1, 2, \ldots$ $2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 64 \not\equiv 1 (\operatorname{mod} 27)$ et $2^9 \equiv (2^3)^3 \equiv 8^3 \equiv (-1)^3 \equiv -1 \not\equiv 1 (\operatorname{mod} 9) \Rightarrow 2^9 \not\equiv 1 (\operatorname{mod} 27)$. Donc 2 est un générateur.

Remarque. Un générateur dans la partie d'arithmétique pour $n \in \mathbb{N}_{>1}$ $\Leftrightarrow$ un générateur de $(\mathbb{Z}/n\,\mathbb{Z})^*$. Et $\operatorname{ord}_n(a) = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^*}(a \pmod{n})$.

En général, pour $n \in \mathbb{N}_{>1}$, on doit tester $a = 2, 3, \ldots$ (il faut que $\operatorname{pgcd}(a, n) = 1$) pour trouver un générateur. Nous remarquons que $\operatorname{ord}_n(a) \mid \varphi(n)$, parce que $\operatorname{pgcd}(a, n) = 1$ et $a^{\varphi(n)} \equiv 1 (\operatorname{mod} n)$. Donc a est un générateur ssi $\operatorname{ord}_n(a) = \varphi(n)$ ssi pour tout premier $p \mid \varphi(n)$, on a $a^{\varphi(n)/p} \not\equiv 1 (\operatorname{mod} n)$. Donc il suffit de

1. Énumérer tous les diviseurs premiers p de $\varphi(n)$.
2. Évaluer $a^{\varphi(n)/p} \bmod n$.
3. a est un générateur ssi $a^{\varphi(n)/p} \not\equiv 1 (\operatorname{mod} n)$ pour tout p au-dessus.

pour déterminer si a est un générateur.

En effet, il y a un théorème:

Théorème. *$(\mathbb{Z}/n\,\mathbb{Z})^*$ admet un générateur ssi n est de forme $1, 2, 4, p^r$ ou $2\,p^r$.*

On a vu que pour évaluer une puissance $a^m (\operatorname{mod} n)$, on peut utiliser le théorème d'Euler ou on factorise $n = p_1^{r_1} \times \cdots \times p_s^{r_s}$ et on utilise le théorème d'Euler pour tout $p_i^{r_i}$. Ici, si $n = 1, 2, 4, p^r, 2\,p^r$, cela ne simplifie rien. C'est-à-dire, ici, il n'y a pas de truc pour simplifier l'évaluation de $a^{\varphi(n)/p} (\operatorname{mod} n)$.

Définition. (Anneaux commutatifs, anneaux intègres $(m \neq 0, n \neq 0 \Longrightarrow m\,n \neq 0)$)

Exemple. (Basiques) Les anneaux suivants sont intègres

1. $k \subseteq \mathbb{C}$ est un sous-corps de $\mathbb{C}$, alors k est un anneau (commutatif). Par exemple, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux.
2. $\mathbb{Z} \subseteq \mathbb{C}$ est un anneau.
3. Anneaux des polynômes: $\mathbb{Z}[X_1, \ldots, X_n]$, $\mathbb{Q}[X_1, \ldots, X_n]$, $\mathbb{R}[X_1, \ldots, X_n]$, $\mathbb{C}[X_1, \ldots, X_n]$.
4. $\mathbb{Z}/p\,\mathbb{Z}$ où p est un premier

Anneaux non-intègres:

1. $\mathbb{Z}/p\,q\,\mathbb{Z}$ où p, q sont deux premiers (pas nécessairement distincts).

Exemple. (Plus compliquée)

1. On a vu dans le CC que $(\mathbb{Z}[1/p], +) \subseteq (\mathbb{Q}, +)$ est un sous-groupe. En effet, $\mathbb{Z}[1/p] = \{m/p^r \mid m \in \mathbb{Z}, r \in \mathbb{N}\} \subseteq \mathbb{Q}$ est un sous-anneau.
2. Plus généralement, $\mathbb{Z}[1/n] = \{m/n^r \mid m \in \mathbb{Z}, r \in \mathbb{N}\} \subseteq \mathbb{Q}$ est un sous-anneau pour tout $n \in \mathbb{N}_{>0}$.

Définition. (Morphismes d'anneaux)

Exemple.

1. Pour tout $(a_1,\ldots,a_n) \in \mathbb{Z}^n$, un morphisme $\mathbb{Z}[X_1,\ldots,X_n] \to \mathbb{Z}$ d'anneaux défini par $\mathbb{Z}[X_1,\ldots,X_n] \ni f \mapsto f(a_1,\ldots,a_n) \in \mathbb{Z}$. En particulier, $\mathbb{Z}[X_1,\ldots,X_n] \to \mathbb{Z}, \sum_{\alpha_1,\ldots,\alpha_n \in \mathbb{N}} c_{\alpha_1,\ldots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n} = f \mapsto f(0,\ldots,0) = c_{0,\ldots,0}$ est un morphisme d'anneaux. Plus conrètement, quand $n = 1$, on a $\mathbb{Z}[X] \to \mathbb{Z}$, $f = c_0 + c_1\,X + \cdots + c_m\,X^m \mapsto c_0 \in \mathbb{Z}$ est un morphisme d'anneaux.
2. On peut remplacer $\mathbb{Z}$ par $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. Pour tout $m, n \in \mathbb{N}_{>0}$, si $m \mid n$, alors il existe un morphisme canonique $\mathbb{Z}/n\,\mathbb{Z} \to \mathbb{Z}/m\,\mathbb{Z}, a(\mathrm{mod}\, n) \mapsto a(\mathrm{mod}\, m)$.
4. Pour tout $m, n \in \mathbb{N}_{>0}$, alors le morphisme $\mathbb{Z}/m\,n\,\mathbb{Z} \to \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z}$ de groupes défini par $a(\mathrm{mod}\, m\,n) \mapsto (a(\mathrm{mod}\, m), a(\mathrm{mod}\, n))$ est effectivement un morphisme d'anneaux. Quand $\mathrm{pgcd}(m, n) = 1$, alors c'est un isomorphisme par le théorème des restes chinois.

Exercice. (TD6 Ex3) Soit A un anneau. Décrire tous les morphismes d'anneaux $\mathbb{Z} \to A$.

Solution. Pour tout morphisme $f : \mathbb{Z} \to A$, on a $f(1) = 1_A$. Alors comme f est un morphisme de groupes, on a $f(n) = n\,1_A$ pour tout $n \in \mathbb{Z}$. Donc il y a au plus un morphisme $\mathbb{Z} \to A$. En revanche, on peut vérifier que $\mathbb{Z} \to A, n \mapsto n\,1_A$ est un morphisme d'anneaux: $f(m+n) = (m+n)\,1_A = m\,1_A + n\,1_A = f(m) + f(n)$, $f(m\,n) = m\,n\,1_A = m\,1_A\,n\,1_A = f(m)\,f(n)$, $f(1) = 1_A$.

Exercice. (TD6 Ex5) Soit A un anneau. Décrire tous les morphismes d'anneaux $\mathbb{Q} \to A$.

Solution. Pour tout morphisme $f : \mathbb{Q} \to A$, comme l'exercice précédent, on a $f(n) = n\,1_A$ pour tout $n \in \mathbb{Z}$. Alors pour tout $m \in \mathbb{Z} \setminus \{0\}$, on a $f(m)\,f(1/m) = f(m\,1/m) = f(1) = 1_A$, donc $m\,1_A = f(m)$ est inversible pour tout $m \in \mathbb{Z} \setminus \{0\}$. Donc

1. Il existe un entier $m \in \mathbb{Z} \setminus \{0\}$ t.q. $m\,1_A$ n'est pas inversible, alors il n'y a aucun morphisme $\mathbb{Q} \to A$ d'anneaux.
2. Sinon, pour tout $m \in \mathbb{Z} \setminus \{0\}$, on a $m\,1_A$ est inversible. Alors pour tout $r \in \mathbb{Q}$, on écrit $r = m/n$ où $m \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$, d'autant que f est un morphisme d'anneaux, $f(n)\,f(r) = f(m) = m\,1_A$ (je vous rappelle que $m\,1_A = 1_A + \cdots + 1_A$ quand $m \geq 0$ et $m\,1_A = -1_A - \cdots - 1_A$ quand $m < 0$) et $f(n) = n\,1_A \in A$ est inversible, alors $f(m/n) = m\,1_A\,(n\,1_A)^{-1} = m\,(n\,1_A)^{-1}$ (la raison: les applications $\mathbb{Z} \to A$ définies par $m \mapsto m\,(n\,1_A)^{-1}$ et $m \mapsto m\,1_A\,(n\,1_A)^{-1}$ sont les morphismes de groupes et les valeurs sont égales quand $m = 1$). Donc il y a au plus un morphisme $\mathbb{Q} \to A$. Dans ce cas, on peut vérifier que l'application $f : \mathbb{Q} \to A$ définie par $m/n \mapsto m\,(n\,1_A)^{-1}$ est bien définie (c'est-à-dire, si $m/n = m'/n'$, alors $m\,(n\,1_A)^{-1} = m'\,(n\,1_A)^{-1}$), et que f est un morphisme d'anneaux:

$$\begin{aligned} f\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) &= f\left(\frac{m_1\,n_2 + m_2\,n_1}{n_1\,n_2}\right) \\ &= (m_1\,n_2 + m_2\,n_1)\,(n_1\,n_2\,1_A)^{-1} \\ f\left(\frac{m_1}{n_1}\right) + f\left(\frac{m_2}{n_2}\right) &= m_1\,(n_1\,1_A)^{-1} + m_2\,(n_2\,1_A)^{-1} \end{aligned}$$

$$
\begin{aligned}
&= m_1\,(n_2\,1_A)\,(n_2\,1_A)^{-1}\,(n_1\,1_A)^{-1} + m_2\,1_A\,(n_2\,1_A)^{-1}\,(n_1\,1_A)^{-1}\,(n_1\,1_A)\\
&= m_1\,n_2\,(n_1\,n_2\,1_A)^{-1} + m_2\,(n_1\,n_2\,1_A)^{-1}\,(n_1\,1_A)\\
&= m_1\,n_2\,(n_1\,n_2\,1_A)^{-1} + n_1\,m_2\,(n_1\,n_2\,1_A)^{-1}\\
&= (m_1\,n_2 + n_1\,m_2)\,(n_1\,n_2\,1_A)^{-1}
\end{aligned}
$$

Donc $f(m_1/n_1 + m_2/n_2) = f(m_1/n_1) + f(m_2/n_2)$. On peut aussi vérifier que $f(m_1/n_1\,m_2/n_2) = f(m_1/n_1)\,f(m_2/n_2)$.

16 Séance 6 jan 2021

Exercice. (TD6, Ex11.1&2) Montrer que $\mathbb{Q}+\mathbb{Q}\sqrt{6}\subseteq\mathbb{R}$ est un sous-anneau ($\mathbb{Q}+\mathbb{Q}\sqrt{6}=\{a+b\sqrt{6}\mid a,b\in\mathbb{Q}\}$), et un élément quelconque de A s'écrit d'une manière unique $a+b\sqrt{6}$ où $a,b\in\mathbb{Q}$.

Solution. $0,1\in\mathbb{Q}+\mathbb{Q}\sqrt{6}$. Pour tout $a,b,c,d\in\mathbb{Q}$, on a $(a+b\sqrt{6})+(c+d\sqrt{6})=(a+c)+(b+d)\sqrt{6}\in\mathbb{Q}+\mathbb{Q}\sqrt{6}$ et $(a+b\sqrt{6})(c+d\sqrt{6})=(ac+6bd)+(bc+ad)\sqrt{6}\in\mathbb{Q}+\mathbb{Q}\sqrt{6}$. Donc $\mathbb{Q}+\mathbb{Q}\sqrt{6}$ est un sous-anneau de $\mathbb{R}$.

Considérons l'application $f:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}+\mathbb{Q}\sqrt{6},(a,b)\mapsto a+b\sqrt{6}$. C'est un morphisme de groupes. Pour montrer que f est injectif, il suffit montrer que $\mathrm{Ker}(f)=0$, c'est-à-dire, si $a+b\sqrt{6}=0$, alors $a=b=0$. Si $b\neq0$, alors $\sqrt{6}=-a/b$, ce qui est impossible ($\sqrt{6}\notin\mathbb{Q}$ un exercice dans la partie d'arithmétique). Alors $b=0$ et donc $a=0$.

Exercice. (TD6, Ex1) Montrer que si $f:A\to B$ est un morphisme d'anneaux, alors on a $f(A^*)\subseteq B^*$ et $f(a^{-1})=f(a)^{-1}$ pour tout $a\in A^*$.

Solution. Il faut montrer que, pour tout $a\in A^*$, alors on a $f(a)^{-1}=f(a^{-1})$, et par conséquent, $f(a)\in B^*$. Il faut vérifier que $f(a)\,f(a^{-1})=f(a^{-1})\,f(a)=1_B$. Comme f est un morphisme d'anneaux, on a $f(a)\,f(a^{-1})=f(a\,a^{-1})=f(1_A)=1_B$, $f(a^{-1})\,f(a)=f(a^{-1}a)=f(1_A)=1_B$. Donc $f(a^{-1})$ est l'inverse de $f(a)$ dans B.

Exercice. (TD6, Ex7) Soit A un anneau. Décrire tous les morphismes d'anneaux $\mathbb{Z}[X]\to A$.

Solution. Pour tout morphisme $f:\mathbb{Z}[X]\to A$, on remarque que $X\in\mathbb{Z}[X]$, alors $f(X)\in A$. On prend $y:=f(X)$. Alors pour tout $\sum_{k=0}^n a_kX^k\in\mathbb{Z}[X]$, on a $f(\sum_{k=0}^n a_kX^k)=\sum_{k=0}^n a_kf(X)^k=\sum_{k=0}^n a_ky^k$.

Ensuite, pour tout $y\in A$, il existe un morphisme d'anneaux $f:\mathbb{Z}[X]\to A$ t.q. $f(X)=y$. En effet, on peut prendre $f(\sum_{k=0}^n a_kX^k)=\sum_{k=0}^n a_ky^k$. On peut vérifier que c'est bien définie, et que c'est un morphisme d'anneaux, c'est-à-dire, pour tout $P,Q\in\mathbb{Z}[X]$, on a $f(P+Q)=f(P)+f(Q)$, $f(PQ)=f(P)\,f(Q)$, $f(1)=1_A$.

En résumé, il y a deux applications $\varphi:\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Z}[X],A):=\{\text{morphismes } f:\mathbb{Z}[X]\to A\}\to A, f\mapsto f(X)$ et $\psi:A\to\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Z}[X],A), y\mapsto(\sum_k a_kX^k\mapsto\sum_k a_ky^k)$, et $\varphi\circ\psi=\mathrm{id}_A$, $\psi\circ\varphi=\mathrm{id}_{\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Z}[X],A)}$, donc φ est une bijection.

Remarque. Un morphisme de groupes $f:G\to H$ est une application f t.q. $f(ab)=f(a)\,f(b)$. Alors prenons $a=b=1_G$, on a $f(1_G)=f(1_G)\,f(1_G)$, donc $1_H=f(1_G)^{-1}\,f(1_G)=f(1_G)^{-1}\,f(1_G)\,f(1_G)=f(1_G)$. C'est-à-dire, pour tout morphisme de groupe $f:G\to H$, on a $f(1_G)=1_H$.

Alors pour tout morphisme d'anneaux $f:A\to B$, f est un morphisme de groupes $(A,+)\to(B,+)$, donc a fortiori $f(0)=0$.

Remarque. Si on remplace $\mathbb{Z}[X]$ par $\mathbb{Q}[X]$, s'il existe un entier $n\in\mathbb{N}_{>0}$ t.q. $n\,1_A$ n'est pas inversible, alors $\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Q}[X],A)=\varnothing$, c'est-à-dire, il n'y aucun morphisme $\mathbb{Q}[X]\to A$ d'anneaux. En revanche, si pour tout $n\in\mathbb{N}_{>0}$, on a $n\,1_A$ est inversible, alors il existe une bijection $\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Q}[X],A)\to A, f\mapsto f(X)$ dont l'inverse et donné par $A\to\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{Q}[X],A), y\mapsto\left(\sum_{k=0}^n\frac{a_k}{b_k}X^k\mapsto(b_k\,1_A)^{-1}a_k\,y^k\right)$.

Exercice. (TD6, Ex6) $\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{R},\mathbb{R})=\{\mathrm{id}_{\mathbb{R}}\}$.

Solution. Tout d'abord, $\mathrm{id}_{\mathbb{R}}:\mathbb{R}\to\mathbb{R}$ est un morphisme d'anneaux. Pour tout morphisme d'anneaux $f:\mathbb{R}\to\mathbb{R}$, on note $E:=\{x\in\mathbb{R}\mid f(x)=x\}$.

1. $0,1\in E$.
2. Si $x,y\in E$, alors $x+y\in E$ et $-x\in E$, c'est-à-dire, $E\subseteq\mathbb{R}$ est un sous-groupe. En effet, $E=\mathrm{Ker}(f-\mathrm{id}_{\mathbb{R}})$ où $f-\mathrm{id}_{\mathbb{R}}:\mathbb{R}\to\mathbb{R},x\mapsto f(x)-x$ est un morphisme de groupes.
3. Pour tout $n\in\mathbb{N}_{>0}$, on a $f(1/n)=1/f(n)=1/n$, donc $1/n\in E$.
4. $\mathbb{Q}\subseteq E$.
5. Pour tout $x\in\mathbb{R}_{\geq0}$, on a $f(x)=f(\sqrt{x}\sqrt{x})=f(\sqrt{x})\,f(\sqrt{x})=f(\sqrt{x})^2\geq0$ (ici, c'est une propriété pariculière de $\mathbb{R}$). Alors pour tout $x,y\in\mathbb{R}$, si $x\leq y$, alors $f(y)=f(x)+f(y-x)\geq f(x)+0=f(x)$.
6. Pour tout $x\in\mathbb{R}$, on a $x\in E$: pour tout $(r,s)\in\mathbb{Q}\times\mathbb{Q}$ t.q. $r\leq x\leq s$, on a $r=f(r)\leq f(x)\leq f(s)=s$. Donc $f(x)=x$ ($\mathbb{Q}\subseteq\mathbb{R}$ est dense).

Corollaire. *Il y a une bijection* $\mathrm{Hom}_{\mathrm{Anneau}}(\mathbb{R}[X],\mathbb{R})\to\mathbb{R}$, $f\mapsto f(X)$ *(parce que pour tout morphisme* $f:\mathbb{R}[X]\to\mathbb{R}$ *d'anneaux, on a* $\mathbb{R}\to\mathbb{R}[X]\xrightarrow{f}\mathbb{R}$ *est un morphisme d'anneaux, alors c'est* $\mathrm{id}_{\mathbb{R}}$*, alors* $f(\sum_k a_k X^k)=\sum a_k f(X)^k$*).*

Définition. (Idéaux) A*: anneau.* $I\subseteq A$ *sous-groupe t.q. pour tout* $a\in A, x\in I$ *on a* $a\,x\in I$ *et* $x\,a\in I$*.*

Exemple. Idéaux de $\mathbb{Z}$. De la forme (n): Tout idéal de $\mathbb{Z}$ est engendré par un élément

Exercice. (TD6, Ex9) Écrire les idéaux suivants de $\mathbb{Z}$ sous la forme $(m)=m\,\mathbb{Z}$: $(10,12)=(10)+(12)$, $(10)\cap(12)$, $(10)\cdot(12)$.

Solution. En générale, pour tout $m,n\in\mathbb{Z}$, on a $(m,n)=(m)+(n)=(\mathrm{pgcd}(m,n))$: vous avez une rélation de Bézout $\mathrm{pgcd}(m,n)\in(m,n)=m\,\mathbb{Z}+n\,\mathbb{Z}$. En revanche, d'autant que $\mathrm{pgcd}(m,n)\mid m$, alors $m\in(\mathrm{pgcd}(m,n))$. Parallèlement $n\in(\mathrm{pgcd}(m,n))$, alors $(m,n)\subseteq(\mathrm{pgcd}(m,n))$.

En particulier, $(10,12)=(\mathrm{pgcd}(10,12))=(2)$.

Pour tout $m,n\in\mathbb{Z}$, on a $(m)\cap(n)=(\mathrm{ppcm}(m,n))$: Quand $m=0$ ou $n=0$, c'est trivial. On suppose que $m\neq0$ et $n\neq0$. Tout d'abord, $\mathrm{ppcm}(m,n)\in(m)$ et $\mathrm{ppcm}(m,n)\in(n)$. Ensuite, si $x\in(m)\cap(n)$, alors il existe $y,z\in\mathbb{Z}$ t.q. $m\,y=n\,z=x$. On prend $m_1=m/\mathrm{pgcd}(m,n)$ et $n_1=n/\mathrm{pgcd}(m,n)$. Alors $m_1\,y=n_1\,z$. Par le lemme d'Euclide, $n_1\mid y$. Donc on peut écrire $y=n_1\,y_1$ où $y_1\in\mathbb{Z}$, alors $x=m\,y=m\,n_1\,y_1=\mathrm{ppcm}(m,n)\,y_1\in(\mathrm{ppcm}(m,n))$.

En particulier, $(10)\cap(12)=(\mathrm{ppcm}(10,12))=(60)$.

Exercice. (TD6, Ex10) Décrire tous les idéaux d'un corps K.

Solution. Tout d'abord, (0) et K sont deux idéaux de K. Ensuite, si $I\subseteq K$ est un idéale qui contient un élément $x\in I$ t.q. $x\neq0$, alors $x^{-1}\in K$, donc $1_K=x^{-1}\,x\in K$ donc $I\supseteq(1_K)=K\Longrightarrow I=K$. En résumé, il n'y a que deux idéaux.

Exercice. (TD6, Ex8) Montrer que si $f:A\to B$ est un morphisme d'anneaux, où A est un corps et $B\neq\{0\}$, alors f est injectif.

Solution. $\mathrm{Ker}(f)\subseteq A$ est un idéale, A est un corps, alors $\mathrm{Ker}(f)=(0)$ ou A. Comme $B\neq\{0\}$, $f(1_A)=1_B\neq0$, alors $\mathrm{Ker}(f)\neq A$. Donc $\mathrm{Ker}(f)=(0)$, c'est-à-dire, f est injectif.

17 Séance 11 jan 2021

Proposition. (Important à mémoriser) *Soit* $n \in \mathbb{N}_{>0}$. $\mathbb{Z}/n\mathbb{Z}$ *corps* $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ *intègre* $\Leftrightarrow$ $n = p$ *premier*

Définition. (Caractéristiques) *Soit* A *un anneau. Il existe un morphisme unique* $f : \mathbb{Z} \to A$. $\mathrm{Ker}(f) = (n)$ *où* $n \in \mathbb{N}$. *Alors* $\mathrm{car}(A) := n$ *est le* caractéristique *de* A.

En particulier, si A est un corps, alors $\mathbb{Z}/\mathrm{Ker}(f) \hookrightarrow A$, donc $\mathbb{Z}/\mathrm{Ker}(f)$ est intègre, donc le caractéristique $\mathrm{car}(A)$ est premier.

Proposition. *Soient* k *un corps et* $f \in k[T] \setminus \{0\}$ *un polynôme.* $k[T]/(f)$ *corps* $\Leftrightarrow$ $k[T]/(f)$ *intègre* $\Leftrightarrow$ f *non-constant, irréductible.*

Théorème. (th des restes chinois) *Soient* k *un corps et* $f, g \in k[T]$ *deux polynômes. Alors on a un morphisme* $k[T]/(fg) \to k[T]/(f) \times k[T]/(g)$. *Si* $\mathrm{pgcd}(f, g) = 1$, *alors c'est un isomorphisme.*

Problème. (Important!) Soient k un corps et $f \in k[T] \setminus \{0\}$ un polynôme.

1. En utilisant le théorème des restes chionois, analyser l'anneau $k[T]/(f)$.
2. En particulier, quand $\deg f \leq 3$, factoriser f.
3. Déterminer $\dim_k(k[T]/(f)) = \deg f$. Quand le cardinal $\#k < \infty$, déterminer $\#(k[T]/(f)) = (\#k)^{\dim_k(k[T]/(f))} = (\#k)^{\deg f}$.
4. Évaluer $T^m \pmod f$ dans $k[T]/(f)$.
5. **(Facultatif)** Déterminer les ordres des élementas de $k[T]/(f)$.

Solution.

1. Tout d'abord, on factorise $f = f_1^{r_1} \cdots f_s^{r_s}$ où $f_1, \ldots, f_s$ sont des polynômes non-constants irréductibles. Alors par le th des restes chinois, l'anneau $k[T]/(f) \cong k[T]/(f_1^{r_1}) \times \cdots \times k[T]/(f_s^{r_s})$. On remarque que si $r_i = 1$, alors $k[T]/(f_i^{r_i})$ est un corps ($\Leftrightarrow$ un anneau intègre).

   En particulier, quand $r_1 = r_2 = \cdots = r_s = 1$, si k est un sous-corps de $\mathbb{C}$, alors il existe un sous-corps $K_i \subseteq \mathbb{C}$ t.q. $k[T]/(f_i) \cong K_i$. En effet, il existe une racine $\xi_i \in \mathbb{C}$ t.q. $f_i(\xi_i) = 0$, alors on prend $K_i = k[\xi_i]$, et l'isomorphisme $k[T]/(f_i) \cong K_i$ (Voir la preuve de TD7, Ex8. Il faut reproduire la preuve dans l'examen) est donné par $T \pmod{f_i} \mapsto \xi_i$, i.e., $g \pmod{f_i} \mapsto g(\xi_i)$ où $g \in k[T]$.

   Les cas particuliers:

   a. Quand $\deg f_i = 1$, alors $\xi_i \in k$ (en effet, $f_i(T) = \alpha_i T + \beta_i$ où $\alpha_i, \beta_i \in k$ et $\alpha_i \neq 0$, alors $\xi_i = -\beta_i/\alpha_i \in k$). Donc $K_i = k$.

   b. Quand $\deg f_i = 2$, alors $K_i = k[\xi_i] := k + k\,\xi_i$.

   En résumé, $k[T]/(f) \cong K_1 \times \cdots \times K_s$ (quand $r_1 = \cdots = r_s = 1$) et un isomorphisme **explicite est donné par** $g \pmod f \mapsto (g(\xi_1), g(\xi_2), \ldots, g(\xi_s))$.

2. On remarque que pour tout non-constant $f \in k[T], \deg f \leq 3$. Si f n'admet aucune racine dans k, alors f est irréductible. En effet, si $f = f_1\, f_2$ où $\deg f_1, \deg f_2 \geq 1$, alors $\deg f = \deg f_1 + \deg f_2$, alors $\min\{\deg f_1, \deg f_2\} \leq 1$, alors f admet une racine dans k.

   Remarque. Si l'on a trouvé une racine α de $f \in k[T]$, alors f se factorise comme $f = (T - \alpha)\, g$ où $g \in k[T]$. Il faut alors trouver $g \in k[T]$ par la division euclidienne. Dans ce cas, il s'agit de la division de f par $T - \alpha$. On peut former le tableau au-dessous. $f(x) = \sum_{k=0}^{n} a_k T^k$

α	a_n	a_{n-1}	a_{n-2}	$\cdots$	$*$	a_i	$\cdots$	a_1	a_0
		$\alpha\, a_n$	$\alpha\, a_{n-1} + \alpha^2\, a_n$	$\cdots$	$*$	$\alpha\, \beta_i$	$\cdots$		
	a_n	$a_{n-1} + \alpha\, a_n$	$a_{n-2} + \alpha\, a_{n-1} + \alpha^2 + a_n$	$\cdots$	β_i	$a_i + \alpha\, \beta_i$	$\cdots$	β_0	$a_0 + \alpha\, a_1 + \alpha^2\, a_2 + \cdots + \alpha^n\, a_n = f(\alpha)$

$$f(T) = (T - \alpha)\,(a_n T^{n-1} + (a_{n-1} + \alpha\, a_n)\, T^{n-2} + \cdots + \beta_0) + a_0 + \alpha\, a_1 + \alpha^2\, a_2 + \cdots + \alpha^n\, a_n$$

Exercice. (TD7 Ex12) Définir un isomorphisme d'anneaux $\mathbb{R}[X]/(X^4-1) \xrightarrow{\sim} \mathbb{R}\times\mathbb{R}\times\mathbb{C}$.

Solution. Tout d'abord, on factorise $X^4-1=(X-1)(X+1)(X^2+1)$. Alors $\mathbb{R}[X]/(X^4-1)\cong\mathbb{R}[X]/(X-1)\times\mathbb{R}[X]/(X+1)\times\mathbb{R}[X]/(X^2+1)$. $\mathbb{R}[X]/(X-1)\xrightarrow{\sim}\mathbb{R}, X(\mathrm{mod}\,(X-1))\mapsto 1$ et $\mathbb{R}[X]/(X+1)\xrightarrow{\sim}\mathbb{R}, X(\mathrm{mod}\,(X+1))\mapsto -1$, $\mathbb{R}[X]/(X^2+1)\xrightarrow{\sim}\mathbb{R}[\mathrm{i}]=\mathbb{R}+\mathrm{i}\,\mathbb{R}=\mathbb{C}$. Donc $\mathbb{R}[X]/(X^4-1)\cong\mathbb{R}\times\mathbb{R}\times\mathbb{C}$, et l'isomorphisme est donné par $\mathbb{R}[X]/(X^4-1)\to\mathbb{R}\times\mathbb{R}\times\mathbb{C}, g\,(\mathrm{mod}\,(X^4-1))\mapsto(g(1),g(-1),g(\mathrm{i}))$.

Exercice. (TD7 Ex14.1) Montrer que $\mathbb{F}_3[X]/(X^3-X+1)$ est un corps.

Solution. C'est un corps ssi X^3-X+1 est irréductible dans $\mathbb{F}_3[X]$, ss'il n'y aucune racine de X^3-X+1 dans $\mathbb{F}_3$ ($\deg(X^3-X+1)\leq 3$). C'est vrai: soit on essaie $X=0,1,2$, ou bien, $a^p-a\equiv 0(\mathrm{mod}\,p)$ (quand $p\nmid a$, par le th de Fermat. quand $p\mid a$, c'est direct).

Exercice. (TD7 Ex14.2) Soit $f=X^3-X+1\in\mathbb{F}_3[X]$. On note $K=\mathbb{F}_3[X]/(f)$. Quels sont les ordres possibles des éléments de K^*?

Solution. On a vu que K est un corps, et K^* est fini, donc K^* est cyclique. On détermine l'ordre de K^*. En effet, $\#K=(\#\mathbb{F}_3)^{\deg f}=3^3=27$, donc $\#K^*=\#K-1=26$. Alors K^* est isomorphe au groupe cyclique $\mathbb{Z}/26\,\mathbb{Z}$, donc tous les ordres possibles des éléments de K^* sont tous les diviseurs positifs de 26, c'est-à-dire, $1,2,13,26$.

Exercice. (TD7 Ex16) Analyser $\mathbb{F}_7[X]/(X^2-X+1)$.

Solution. X^2-X+1 admet une racine 3 dans $\mathbb{F}_7$, alors $X^2-X+1=(X-3)(X+2)$, donc $\mathbb{F}_7[X]/(X^2-X+1)\xrightarrow{\sim}\mathbb{F}_7\times\mathbb{F}_7$ et l'isomorphisme est donné par $f(\mathrm{mod}\,(X^2-X+1))\mapsto(f(3),f(-2))$.

Remarque. Pour faire la division euclidienne X^2-X+1 par $X-3$, le résultat est $X+2$

3	1	−1	1
		3	6
	1	2	7 = 0

18 Séance 13 jan 2021

Problème. (Important!) Soient k un corps et $f \in k[T] \setminus \{0\}$ un polynôme.

1. Évaluer $T^m \pmod f$ (ou plus généralement, $g(T) \pmod f$ où $g \in k[T]$) dans $k[T]/(f)$ (On peut le simplifier seulement quand $m < \deg f$ (ou respectivement $\deg g < \deg f$))
2. **(Facultatif)** Déterminer les ordres des élements de $k[T]/(f)$.

Solution. Pour évaluer T^m, il y a quelques trucs:

a) Quand k est fini et f est irréductible (non-constant), $K = k[T]/(f)$ est un corps et $T \pmod f \neq 0$, alors $T^{\#K^*} = 1$ où $\#K^* = (\#k)^{\deg f} - 1$. Donc on peut tout d'abord remplacer m par $m \bmod (\#K^*)$.

b) En général, on suppose que f est unitaire, $f = T^n + \sum_{k=0}^{n-1} a_k T^k$. Pour évaluer $T^m \pmod f$, il suffit de faire la division euclidienne T^m par f (vous avez le reste) dans l'anneau $k[T]$ de polynômes.

Alternativement, dans $k[T]/(f)$, on a $T^n \equiv -\sum_{k=0}^{n-1} a_k T^k \pmod f$ (à gauche, T^n, à droite, $T^{\leq n-1}$). Donc $T^m = T^n T^{n-m} = (-\sum_{k=0}^{n-1} a_k T^k) T^{n-m}$ dans $k[T]/(f)$. On continue. En général, cela va être compliqué.

Quand $f = T^n + a_0$, alors cela va être beaucoup simplifié: on écrit $m = n\,q + r$ où $q, r \in \mathbb{Z}, 0 \leq r < n$, alors $T^m = (T^n)^q T^r \equiv (-a_0)^q T^r \pmod f$.

Exercice. (TD7 Ex8) Montrer que l'anneau $A = \mathbb{Q} + \mathbb{Q}\sqrt{6}$ est isomorphe à $\mathbb{Q}[X]/(X^2 - 6)$.

Solution. Tout d'abord, il existe un morphisme d'anneau $f : \mathbb{Q}[X] \to A, X \mapsto \sqrt{6}$ (morphisme d'évaluation). Par définition, f est surjectif, $X^2 - 6 \in \mathrm{Ker}(f)$, donc on a un morphisme (composé) d'anneau $g : \mathbb{Q}[X]/(X^2-6) \to \mathbb{Q}[X]/\mathrm{Ker}(f) \xrightarrow{\simeq} A$. Il suffit de montrer que g est un isomorphisme.

Comme $X^2 - 6$ est irréductible dans $\mathbb{Q}[X]$ (parce que $X^2 - 6$ n'admet aucune racine dans $\mathbb{Q}$), $\mathbb{Q}[X]/(X^2-6)$ est un corps. Par TD6, Ex8, g est injectif. De l'autre côté, g est le morphisme composé $\mathbb{Q}[X]/(X^2-6) \to \mathbb{Q}[X]/\mathrm{Ker}(f) \xrightarrow{\simeq} A$, g est surjectif. En résumé, g est un isomorphisme.

Exercice. (TD7 Ex18.2) Montrer que $K = \mathbb{F}_7[X]/(X^3 - 2)$ est un corps. Quels sont les ordres possibles des éléments de K^*? Quel est l'ordre de la classe $\alpha = X \pmod{X^3-2} \in K^*$ (c'est-à-dire, l'image de X par l'appli $\mathbb{F}_7[X] \twoheadrightarrow \mathbb{F}_7[X]/(X^3-2)$).

Solution. Pour montrer que K est un corps, il suffit de montrer que $X^3 - 2$ est irréductible dans $\mathbb{F}_7[X]$. Comme $\deg(X^3 - 2) = 3 \leq 3$, il suffit de vérifier que $X^3 - 2$ n'admet aucune racine dans $\mathbb{F}_7$, ce qui peut être vérifié par évaluant $\beta^3 - 2$ pour $\beta = 0, \pm 1, \pm 2, \pm 3$ (alternativement, s'il existe $\beta \in \mathbb{F}_7$ t.q. $\beta^3 = 2$, alors $\beta \neq 0$ et donc par le th d'Euler, $\beta^6 = 1$ mais $\beta^6 = (\beta^3)^2 = 4 \neq 1$ dans $\mathbb{F}_7$). $\dim_{\mathbb{F}_7}(K) = \deg(X^3 - 2) = 3$, alors $\#K = 7^3$ et $\#K^* = \#K - 1 = 7^3 - 1 = 6\,(7^2 + 7 + 1) = 6 \times 57 = 2 \times 3^2 \times 19$. Comme K^* est un groupe cyclique (fini), tous les ordres possibles sont les diviseurs de $\#K^*$: $2^u\,3^v\,19^w$ où $u = 0, 1; v = 0, 1, 2; w = 0, 1$.

Pour déterminer $\mathrm{ord}_{K^*}(\alpha)$, tout d'abord, $\mathrm{ord}_{K^*}(\alpha) \mid \mathrm{ord}(K^*) = 2 \times 3^2 \times 19$. En suite, par définition, $\alpha^3 - 2 = X^3 - 2 \pmod{X^3 - 2} = 0$ dans K, donc $\alpha^3 = 2$. On écrit $\mathrm{ord}_{K^*}(\alpha) = 3\,q + r$ où $q, r \in \mathbb{Z}, 0 \leq r < 3$, alors $1 = \alpha^{\mathrm{ord}_{K^*}(\alpha)} = \alpha^{3q+r} = (\alpha^3)^q\,\alpha^r = 2^q\,\alpha^r$. Comme $r < 3$, on a $r = 0$ (vous avez vu que $\dim_{\mathbb{F}_7}(K) = 3$ et $1, \alpha, \alpha^2$ constitue une base) et $1 = 2^q$ dans $\mathbb{F}_7$, donc $\mathrm{ord}_{\mathbb{F}_7}(2) \mid q$. On peut voir que $\mathrm{ord}_{\mathbb{F}_7}(2) = 3$, donc $3 \mid q \Rightarrow 9 \mid \mathrm{ord}_{K^*}(\alpha)$.

En revanche, $\alpha^9 = (\alpha^3)^3 = 2^3 = 1$ dans K, donc $\mathrm{ord}_{K^*}(\alpha) \mid 9$. En résumé, $\mathrm{ord}_{K^*}(\alpha) = 9$.

Exercice. (TD7 Ex14.3) Soit $f = X^3 - X + 1 \in \mathbb{F}_3[X]$. On note $K = \mathbb{F}_3[X]/(f)$ et $\alpha = X \pmod f \in K$. Montrer que $\alpha^{13} = -1$. En déduire que α est un générateur de K^*. (On a déjà vu que K est un corps, donc $\alpha \in K^*$)

Solution. Par définition, $\alpha^3 = \alpha - 1$ dans K. $\alpha^{13} = (\alpha^3)^4\,\alpha = (\alpha - 1)^4\,\alpha = (\alpha^4 - 4\,\alpha^3 + 6\,\alpha^2 - 4\,\alpha + 1)\,\alpha = (\alpha^4 - \alpha^3 - \alpha + 1)\,\alpha = (\alpha^3\,(\alpha - 1) - (\alpha - 1))\,\alpha = ((\alpha - 1)\,(\alpha - 1) - (\alpha - 1))\,\alpha = \alpha\,(\alpha - 1)\,(\alpha - 2) = \alpha\,(\alpha - 1)\,(\alpha + 1) = \alpha\,(\alpha^2 - 1) = \alpha^3 - \alpha = \alpha - 1 - \alpha = -1$.

On note que $\#K^* = 26$. Pour montrer que α est un générateur, il suffit de montrer que pour tout premier $p \mid 26$, on a $\alpha^{26/p} \neq 1$. $\alpha^{26/2} = \alpha^{13} = -1$ et $\alpha^{26/13} = \alpha^2$. Comme $1, \alpha, \alpha^2$ constitue une base de K comme un $\mathbb{F}_3$-espace vectoriel, $\alpha^2 \neq 1$. Donc α est un générateur.

Remarque. En général, c'est difficile pour trouver un générateur (on a déjà vu qu'il va être difficile en général même pour $\mathbb{F}_p$ quand p est grand).

Exercice. (TD7 Ex15) Montrer que le polynôme $X^2-X-1\in\mathbb{F}_7[X]$ est irréducible dans $\mathbb{F}_7[X]$. En déduire que l'anneau $K=\mathbb{F}_7[X]/(X^2-X-1)$ est un corps. On note $\alpha\in K$ la classe de X. Montrer que $\alpha^{483}=2\,\alpha+1$.

Solution. On vérifie que $\alpha^2-\alpha-1=\alpha\,(\alpha-1)-1\neq 0$ quand $\alpha=0,1,2,3,4,5,6\in\mathbb{F}_7$. Donc il n'y aucune racine de X^2-X-1 dans $\mathbb{F}_7$, donc K est un corps. En particulier, $\alpha\neq 0$ alors $\alpha\in K^*$, donc $\alpha^{\#K^*}=1$ où $\#K^*=\#K-1=7^2-1=6\times 8=48$. Alors $483=48\times 10+3$ et $\alpha^{483}=(\alpha^{48})^{10}\,\alpha^3=\alpha^3=\alpha\,(\alpha+1)=\alpha^2+\alpha=\alpha+1+\alpha=2\,\alpha+1$.

Exercice. (TD7 Ex18.1) Pour quelles valeurs de $a\in\mathbb{F}_7$, le polynôme X^3-a est-il irréductible dans $\mathbb{F}_7[X]$?

Solution. X^3-a est irréductible dans $\mathbb{F}_7[X]$ ssi X^3-a n'admet aucune racine dans $\mathbb{F}_7$ ssi $\alpha^3-a\neq 0$ pour $\alpha=0,\pm1,\pm2,\pm3$.

$$\begin{array}{rccccc}\alpha= & 0 & \pm1 & \pm2 & \pm3\\ \alpha^3= & 0 & \pm1 & \pm1 & \pm1\end{array}$$

Donc X^3-a admet une racine ssi $a=0,\pm1$, c'est-à-dire, X^3-a n'admet aucune racine ssi $a=\pm2,\pm3$.

Exercice. (TD7 Ex2) Factoriser le polynôme X^4+1 dans $\mathbb{R}[X]$.

Solution. Il s'agit de la factorisation d'un polynôme de type $X^4+a\,X^2+1$. On a $X^4+1=(X^2+1)^2-(\sqrt{2}\,X)^2=(X^2-\sqrt{2}\,X+1)\,(X^2+\sqrt{2}\,X+1)$ dans $\mathbb{R}[X]$.

Exercice. (TD7 Ex6.1) Déterminer le nombre de polynômes unitaires de degré 2 dans $\mathbb{F}_p[X]$.

Exercice. (TD7 Ex17) Montrer que le polynôme $X^3-X-2\in\mathbb{F}_5[X]$ est irréductible.

Exercice. (TD7 Ex13) Trouver tous les polynômes unitaires irréductibles $f_j\in\mathbb{F}_2[X]$ de degré $\deg(f_j)=3$. Déterminer le cardinal de $\mathbb{F}_2[X]/(f_j)$.