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

Réponse.

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

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. $36\,a + 126\,b = d \Longleftrightarrow \frac{36}{d}\,a + \frac{126}{d}\,b = 1$ où $\operatorname{pgcd}(36/d, 126/d) = 1$ (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 $d = \operatorname{pgcd}(a, b)$ (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: $4\,x+9\,y=1$, $18\,x+7\,y=2$, $5\,x-18\,y=4$, $6\,x+15\,y=28$, $56\,x+35\,y=14$

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

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

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 $A_n=\left(\begin{smallmatrix} 1 & *\\ & 1\end{smallmatrix}\right)$

3 Séance 26 oct 2020

Exercice. (TD2 Ex10) Soients $a, b, x, y \in \mathbb{Z}$ $(a, b \neq 0)$. 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. $\mathrm{pgcd}(a, b) = d \Longrightarrow \mathrm{pgcd}(a\,c, b\,c) = d\,|c|$.
2. $(\mathrm{pgcd}(a, b) = 1 \text{ et } \mathrm{pgcd}(a, c) = 1) \Longrightarrow \mathrm{pgcd}(a, b\,c) = 1$.
3. $\mathrm{pgcd}(a, b) = 1 \Longrightarrow (\forall m, n \geq 2\colon \mathrm{pgcd}(a^m, b^n) = 1)$.
4. $\mathrm{pgcd}(a, b) = d \Longrightarrow (\forall m \geq 2\colon \mathrm{pgcd}(a^m, b^m) = d^m)$.

Réponse.

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

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 $\operatorname{pgcd}(a,b),\operatorname{ppcm}(a,b)$ 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 $\operatorname{ppcm}(a,b)$ dont une factorisation suffit).

Réponse. Calculons $\operatorname{pgcd}(a,b)$ 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 $\operatorname{pgcd}(a,b)=2$. $\operatorname{ppcm}(a,b)=68\times 42/2$

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

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

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. $\left\{\begin{smallmatrix} 7\,x \equiv 5 \pmod{19} \\ 6\,x \equiv 3 \pmod{15} \end{smallmatrix}\right.$

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 $\left\{\begin{smallmatrix} x \equiv -2 \pmod{19} \\ x \equiv -2 \pmod{5} \end{smallmatrix}\right.$ donc $x \equiv -2 \;(\mathrm{mod}\,95 = \mathrm{ppcm}(19, 5))$

   Remarque 7. En général, pour résoudre un système d'équations $\left\{\begin{smallmatrix} x \equiv c_1 \pmod{a_1} \\ x \equiv c_2 \pmod{a_2} \end{smallmatrix}\right.$, $x = a_1\,y + c_1 = a_2\,z + c_2$ 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 $\left\{\begin{smallmatrix} x \equiv 1 \pmod{a_1} \\ x \equiv 0 \pmod{a_2 \cdots a_n} \end{smallmatrix}\right.$. 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. $\mathrm{pgcd}(a,b)=d \Longrightarrow \left(\forall m,n\geq 2\colon \mathrm{pgcd}\left(\frac{a^m}{d^m},\frac{b^n}{d^n}\right)=1\right)$.

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 $\mathrm{pgcd}(a, b)\, \mathrm{ppcm}(a, b) = |a\, b|$.

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

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 $100^{1000} \equiv 100^4 \equiv (-4)^4 \equiv 16^2 \equiv 3^2 \equiv -4 (\mathrm{mod}\, 13)$.

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 $3 \mid (x^2 + y^2) \Longrightarrow 3 \mid x \text{ et } 3 \mid y \Longrightarrow 9 \mid (x^2 + y^2) \Longrightarrow 9 \mid (3\,z^2) \Longrightarrow 3 \mid z^2 \xRightarrow{(3 \text{ est premier})} 3 \mid z$.
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

$$\left\{\begin{array}{lcl} x & \equiv & 1 \pmod{34} \\ x & \equiv & 0 \pmod{55} \end{array}\right.$$

et

$$\left\{\begin{array}{lcl} x & \equiv & 0 \pmod{34} \\ x & \equiv & 1 \pmod{55} \end{array}\right.$$

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

En déduire la solution de

$$\left\{\begin{array}{lcl} x & \equiv & \alpha \pmod{34} \\ x & \equiv & \beta \pmod{55} \end{array}\right.$$

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

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

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 $13\times 55 \equiv 1 \pmod{34}$ et $13\times 55 \equiv 0 \pmod{55}$ donc $x \equiv 13\times 55 \pmod{34\times 55}$ est une solution du premier système (vous pouvez voir que les étapes ici sont parallèles à celles de $55\,y \equiv 1 \pmod{34}$: 13 est l'inverse de $55 \bmod 34$). Parallèlement, $x \equiv -21\times 34 \pmod{34\times 55}$ est une solution du second système.

Pour la troisième, $x \equiv 13\times 55\,\alpha - 21\times 34\,\beta \pmod{34\times 55}$.

7 Séance 23 nov 2020

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

$$\begin{cases} x & \equiv & 3 \pmod 7 \\ x & \equiv & 1 \pmod 8 \\ x & \equiv & 4 \pmod 9 \end{cases} \tag{5}$$

Solution. Tout d'abord, nous résolvons

$$\begin{cases} x & \equiv & 3 \pmod 7 \\ x & \equiv & 1 \pmod 8 \end{cases}$$

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

Alors le système (5) est équivalent à

$$\begin{cases} x & \equiv & 17 \pmod{7\times 8} \\ x & \equiv & 4 \pmod 9 \end{cases} \tag{6}$$

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: $8^{-1}\equiv(-1)^{-1}\equiv -1 \pmod 9$. 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 $4\times 7\equiv 1 \pmod 9$, cela vaut dire, $7^{-1}\equiv 4 \pmod 9$. Pour résoudre le système (6), on prend $x=17+7\times 8\,y$, alors on a $17+7\times 8\,y\equiv 4 \pmod 9$, cela vaut dire $7\times 8\,y\equiv 5 \pmod 9 \Longrightarrow y\equiv 5\,(7^{-1})\,(8^{-1})\equiv 5\times 4\times(-1)\equiv -2 \pmod 9$. 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 $a \pmod{12}\in(\mathbb{Z}/12\,\mathbb{Z})^\times$. Pour chaque élément de l'ensemble $(\mathbb{Z}/12\,\mathbb{Z})^\times$ determiner son inverse. Idem pour $(\mathbb{Z}/18\,\mathbb{Z})^\times$.

Solution. $a \pmod{12}\in(\mathbb{Z}/12\,\mathbb{Z})^\times$ 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 $a^2\equiv 1 \pmod{12}$, donc $a^{-1}\equiv a \pmod{12}$.

Parallèllement, $a \pmod{18}\in(\mathbb{Z}/18\,\mathbb{Z})^\times$ 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, $a\equiv\pm 1, \pm 5, \pm 7 \pmod{18}$. On peut évaluer un par un $a^{-1} \pmod{18}$. 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 $\operatorname{pgcd}(a, n) = 1$, 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 $\operatorname{pgcd}(a,n)=1$. 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 $2019^{2018}\equiv 17^{2018} \pmod{91}$. $\operatorname{pgcd}(17, 91)=1$. 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 $\operatorname{pgcd}(2,18)=2\neq 1$. 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 $\mathrm{pgcd}(a,6)=1 \Longrightarrow a^2 \equiv 1 \pmod{24}$.
2. Montrer que $a^{13} \equiv a \pmod{2730}$.

Solution.

1. $24 = 2^3 \times 3$. Alors il suffit ($\mathrm{pgcd}(2^3,3)=1$) de montrer que $a^2 \equiv 1 \pmod{2^3}$ et $a^2 \equiv 1 \pmod 3$. D'autant que $\mathrm{pgcd}(2, a)=1$, 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

$$\left\{ \begin{array}{lll} x & \equiv & \alpha \pmod 7 \\ x & \equiv & \beta \pmod{13} \end{array} \right.$$

   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

$$\left\{ \begin{array}{lll} x & \equiv & \alpha \pmod 7 \\ x & \equiv & \beta \pmod{13} \end{array} \right.$$

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 $\mathrm{pgcd}(x, 30) = 1$, 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 $\mathrm{pgcd}(x, 30 = 2 \times 3 \times 5) = 1$, 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 $x^4 \equiv 1 \pmod{\mathrm{ppcm}(2^4, 3, 5) = 240}$.
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 $x^8 \equiv x^4 \pmod{\mathrm{ppcm}(2^4, 3, 5) = 240}$.
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

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 $a^6 \not\equiv 1 (\bmod 27)$ et $a^9 \not\equiv 1 (\bmod 27)$. Donc on teste $a = 1, 2, \ldots$ $2^6 \equiv (2^3)^2 \equiv 8^2 \equiv 64 \not\equiv 1 (\bmod 27)$ et $2^9 \equiv (2^3)^3 \equiv 8^3 \equiv (-1)^3 \equiv -1 \not\equiv 1 (\bmod 9) \Rightarrow 2^9 \not\equiv 1 (\bmod 27)$. 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 $m \nmid (n/p)$.

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

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 $a^{100} \equiv 1 \pmod{1000 = \operatorname{ppcm}(2^3, 5^3)}$.

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: $b^{100} \equiv 0, 1 (\bmod 2^3)$ et $b^{100} \equiv 0, 1 (\bmod 5^3)$. Il suffit de résoudre le système $x \equiv \alpha (\bmod 2^3)$ 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. $x^2 \equiv 1 (\bmod p)$ 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. $x^2 \equiv 1 (\bmod p^r)$ 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 $x+1 \equiv 2 \not\equiv 0 (\bmod p) \Rightarrow p \nmid x+1 \Rightarrow \operatorname{pgcd}(p^r, x+1) = 1 \xRightarrow{p^r \mid (x-1)(x+1)} p^r \mid x-1$. Parallèllement, si $p \mid x+1$ alors on a $p^r \mid x+1$. Conclusions: si $p^r \mid (x-1)(x+1)$, alors $x \equiv \pm 1 \ (\bmod p^r)$. Vérifier que ce sont les solutions.

3. On factorise $91 = 7 \times 13$ et $105 = 3 \times 5 \times 7$. Alors $x^2 \equiv 1 (\bmod 91)$ ssi $x^2 \equiv 1 (\bmod 7)$ et $x^2 \equiv 1 (\bmod 13)$ ssi $x \equiv \pm 1 (\bmod 7)$ et $x \equiv \pm 1 (\bmod 13)$. 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 $\frac{x+1}{2} = \frac{x-1}{2} + 1 \equiv 1 (\bmod 2) \Rightarrow \operatorname{pgcd}\left(2^{r-2}, \frac{x+1}{2}\right) = 1 \xRightarrow{2^{r-2} \mid \frac{x+1}{2} \frac{x-1}{2}} 2^{r-2} \mid \frac{x-1}{2} \Rightarrow 2^{r-1} \mid x-1$. Si $2 \mid \frac{x+1}{2}$, parallèllement, on a $2^{r-1} \mid x+1$. Conclusion: $x \equiv \pm 1 \ (\bmod 2^{r-1} = n/2)$. On peut vérfier que quand $x \equiv \pm 1 (\bmod 2^{r-1})$, on a $x^2 \equiv 1 \ (\bmod n)$.

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

11 Séance 7 déc 2020

Définition. Groupe G: $\mathrm{mult}: G\times G \to G$ *et un élément (neutre)* $e\in G$ *(on va écrire* $\mathrm{mult}(a,b)$ *comme* $a\,b$*) t.q.*

1. $(a\,b)\,c = a\,(b\,c)$ *pour tout* $a,b,c\in G$.
2. $e\,a = a\,e = a$ *pour tout* $a\in G$
3. *Pour tout* $a\in G$*, il existe un inverse* $a^{-1}\in G$ *t.q.* $a\,a^{-1} = a^{-1}\,a = e$.

Si $a\,b = b\,a$ *pour tout* $a,b\in G$*, alors on dit que le groupe* G *est abélien.*

Remarque. L'élément neutre et l'inverse sont en effet unique.

Définition. Sous-groupe $H\subseteq G$

1. $e\in H$
2. *Pour tout* $a,b\in H$*, on a* $a\,b\in H$
3. *Pour tout* $a\in G$*, on a* $a^{-1}\in H$.

Définition. *Un morphisme de groupes* $f: G\to H$*: pour tout* $a,b\in G$*, on a* $f(a\,b) = f(a)\,f(b)$ *(par conséquent,* $f(e) = e$ *et* $f(a^{-1}) = f(a)^{-1}$*). En particulier, si* $H\subseteq G$*, alors l'inclusion* $H\hookrightarrow G$ *est un morphisme de groupes.*

Exercice. (TD5 Ex1) Vrai ou faux: $(\mathbb{N},+)$ (resp. $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Z}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R},\cdot)$, $(2\,\mathbb{Z}+1,+)$) est un groupe.

Solution.

1. $(\mathbb{N},+)$ n'est pas un groupe. Sinon, soit $e\in\mathbb{N}$ l'élément neutre. Alors par définition, on a $e+0=0$ donc $e=0$ (vous pouvez aussi utiliser l'unicité de l'élément neutre pour montrer que si $(\mathbb{N},+)$ est un groupe, alors $0\in\mathbb{N}$ est l'élément neutre). Alors pour tout $x\in\mathbb{N}$, on a $x+1>1\neq 0$ donc il n'y pas d'inverse de $1\in\mathbb{N}$.
2. $(\mathbb{Z},+)$ est un groupe. L'élément neutre: $0\in\mathbb{Z}$. L'inverse d'un élément $x\in\mathbb{Z}$: $-x$.
3. $(\mathbb{Z},\cdot)$ n'est pas un groupe. Sinon, soit $e\in\mathbb{Z}$ l'élément neutre, alors $e\,1 = 1\Rightarrow e=1$. Alors pour tout $x\in\mathbb{N}$, $2\mid 2\,x$, $2\nmid 1\Rightarrow 2\,x\neq 1$, donc 2 n'admet pas d'inverse.
4. $(\mathbb{Z}\setminus\{0\},\cdot)$ n'est pas un groupe. Sinon, soit $e\in\mathbb{Z}$ l'élément neutre, alors $e\,1=1\Rightarrow e=1$. Alors pour tout $x\in\mathbb{N}$, $2\mid 2\,x$, $2\nmid 1\Rightarrow 2\,x\neq 1$, donc 2 n'admet pas d'inverse.
5. $(\mathbb{R}\setminus\{0\},\cdot)$ est un groupe dont l'élément neutre: $1\in\mathbb{R}\setminus\{0\}$, l'inverse de $x\in\mathbb{R}\setminus\{0\}$: x^{-1}.
6. $(\mathbb{R},\cdot)$ n'est pas un groupe. Sinon, soit $e\in\mathbb{Z}$ l'élément neutre, alors $e\,1=1\Rightarrow e=1$. Alors pour tout $x\in\mathbb{R}$, on a $x\,0=0\neq 1$, donc $x\in\mathbb{R}$ n'admet pas d'inverse.
7. $(2\,\mathbb{Z}+1,+)$ (où $2\,\mathbb{Z}+1$ est l'ensemble des impairs). Sinon, $2\,\mathbb{Z}+1$ est un groupe. Quelques méthodes:
   a. $2\,\mathbb{Z}+1\subseteq\mathbb{Z}$ est un sous-groupe, mais $0\in\mathbb{Z}$ est l'élément neutre dans $\mathbb{Z}$, mais $0\notin 2\,\mathbb{Z}+1$, c'est absurde.
   b. $+$ n'est pas bien définie sur $2\,\mathbb{Z}+1$. Par exemple, $1+1=2\notin 2\,\mathbb{Z}+1$.

Exercice. (TD5 Ex2) Montrer que $2\,\mathbb{Z}\subseteq\mathbb{Z}$ est un sous-groupe et que l'app $f:\mathbb{Z}\to 2\,\mathbb{Z}, x\mapsto 2\,x$ est un isomorphisme de groupes.

Solution. Pour montrer que $2\,\mathbb{Z}\subseteq\mathbb{Z}$ (c'est le groupe $(\mathbb{Z},+)$) est un sous-groupe, il suffit de vérifier que

1. L'élément neutre $0\in 2\,\mathbb{Z}$.
2. Si $x,y\in 2\,\mathbb{Z}$, alors $x+y\in 2\,\mathbb{Z}$ (déjà vu dans la partie d'arithmétique)
3. Si $x\in 2\,\mathbb{Z}$, alors $-x\in 2\,\mathbb{Z}$.

Pour montrer que $f:\mathbb{Z}\to 2\,\mathbb{Z}, x\mapsto 2\,x$ est un isomorphisme, il faut montrer tout d'abord que f est un morphisme de groupes, c'est-à-dire, pour tout $x, y\in\mathbb{Z}$, on a $f(x)+f(y)=f(x+y)\Longleftrightarrow 2\,x+2\,y=2\,(x+y)$, c'est vrai. Alors pour montrer que f est un isomorphisme, il suffit de montrer que $\operatorname{Ker}(f)=0$ et f est surjective. Pour tout $x\in\mathbb{Z}$, si $f(x)=0$, alors $2\,x=0\Longrightarrow x=0$. Donc $\operatorname{Ker} f=0$. Pour tout $y\in 2\,\mathbb{Z}$, par définition, il existe $x\in\mathbb{Z}$ t.q. $y=2\,x=f(x)$, donc f est surjective.

Exercice. (TD5 Ex7) Les groupes suivants, sont-ils isomorphes? Pourquoi?

1. $G:=(\mathbb{Z}/4\,\mathbb{Z},+)$ et $H:=(\mathbb{Z}/2\,\mathbb{Z},+)\times(\mathbb{Z}/2\,\mathbb{Z},+)$;

Solution.

1. $G[2]=\{x\in\mathbb{Z}/4\,\mathbb{Z}\mid x+x\equiv 0\,(\operatorname{mod} 4)\}=\{0(\operatorname{mod} 4), 2(\operatorname{mod} 4)\}$. Pour autant, $H[2]=H$, c'est-à-dire, pour tout $x\in H$, on a $x+x=0$ (en effet, pour tout $(x,y)\in\mathbb{Z}/2\,\mathbb{Z}\times\mathbb{Z}/2\,\mathbb{Z}$, on a $(x,y)+(x,y)\xlongequal{\text{déf d'un groupe produit}}(x+x, y+y)=(0(\operatorname{mod} 2), 0(\operatorname{mod} 2))$, alors par définition, $H[2]=H$). Maintenant, $\#G[2]=2$ mais $\#H[2]=\#H=4$ donc $\#G[2]\neq\#H[2]\Longrightarrow G[2]\ncong H[2]\Longrightarrow G\ncong H$.

Remarque 9. Soient G, H deux groupes. Il n'y pas d'algorithme pour déterminer si G et H sont isomorphes. Pour autant, on a quelques trucs pour déterminer si les deux groupes ne sont pas isomorphes:

1. Si G est fini, H est infini, alors G n'est pas isomorphe à H (parce que comme deux ensembles).

2. Si G, H sont finis et $\#G:=\operatorname{Card}(G)\neq\#H$, alors G n'est pas isomorphe à H (parce que comme deux ensembles).

3. Soit G un groupe abélien, $G[n]:=\{g\in G\mid g^n=e\}\subseteq G$ est un sous-groupe (tout d'abord, $e\in G[n]$. Ensuite, si $x, y\in G[n]$, alors $(x\,y)^n\xlongequal{\text{abel}}x^n\,y^n=e\,e=e\Longrightarrow x\,y\in G[n]$. Enfin, si $x\in G[n]$, alors $(x^{-1})^n=(x^n)^{-1}=e^{-1}=e$).

   Soient G, H deux groupes abéliens, alors si G est isomorphe à H par $\varphi:G\to H$, alors pour tout $n\in\mathbb{N}$, $G[n]\cong H[n]$ (parce que $\varphi(G[n])\subseteq H[n]$ cela induit un morphisme $\psi:G[n]\to H[n]$ de groupes. On peut vérifier que $\operatorname{Ker}(\psi)=0$ et $\operatorname{Im}(\psi)=H[n]$, donc ψ est un isomorphisme). Donc si nous pouvons trouver $n\in\mathbb{N}$ t.q. $G[n]\ncong H[n]$, alors $G\ncong H$.

12 Séance 9 déc 2020

Notation. *$G \cong H$ ssi G, H sont isomorphes, et $G \ncong H$ ssi G, H ne sont pas isomorphes.*

Remarque. Soit G un groupe abélien (la notation multiplicative). Alors pour tout $n \in \mathbb{N}$, on a $p_{G,n}: G \to G, g \mapsto g^n$ est un morphisme de groupes ($(g\,h)^n = g^n\,h^n$ abélien). Alors $G[n] = \operatorname{Ker}(p_{G,n}) \subseteq G$ est un sous-groupe. En suite, si $f: G \to H$ est un morphisme de groupes abéliens, alors $f(G[n]) \subseteq H[n]$ parce que pour tout $g \in G$, on a $f(g^n) = f(g)^n$, donc si $g \in G[n] \Longrightarrow g^n = 0$, alors $f(g)^n = 0$, c'est-à-dire, $f(g) \in H[n]$. Si $f: G \to H$ est un isomorphisme, alors $f(G[n]) \subseteq H[n]$, et $f^{-1}: H \to G$, $f^{-1}(H[n]) \subseteq G[n]$. Donc $f|_{G[n]}: G[n] \to H[n]$ et $f^{-1}|_{H[n]}: H[n] \to G[n]$ sont deux morphismes de groupes et $f|_{G[n]} \circ f^{-1}|_{H[n]} = \mathrm{id}_{H[n]}$, $f^{-1}|_{H[n]} \circ f|_{G[n]} = \mathrm{id}_{G[n]}$, donc $G[n] \cong H[n]$.

Question. $(\mathbb{Z}/m\,\mathbb{Z}, +)$ est un groupe dont le cardinal est m. Alors si $m \neq n$, alors $\mathbb{Z}/m\,\mathbb{Z} \ncong \mathbb{Z}/n\,\mathbb{Z}$.

Exercice. (TD5 Ex7) Les groupes suivants, sont-ils isomorphes? Pourquoi? G et H.

1. $(\mathbb{R}, +)$ et $(\mathbb{R}_{>0}, \cdot)$;
2. $(\mathbb{Z}/6\,\mathbb{Z}, +)$ et $(\mathbb{Z}/2\,\mathbb{Z}, +) \times (\mathbb{Z}/3\,\mathbb{Z}, +)$;
3. $(\mathbb{Z}/m\,n\,\mathbb{Z}, +)$ et $(\mathbb{Z}/m\,\mathbb{Z}, +) \times (\mathbb{Z}/n\,\mathbb{Z}, +)$;
4. $(\mathbb{Z}/4\,\mathbb{Z}, +)$ et $((\mathbb{Z}/5\,\mathbb{Z}) \setminus \{0\}, \cdot)$;
5. $(\mathbb{R} \setminus \{0\}, \cdot)$ et $(\mathbb{C} \setminus \{0\}, \cdot)$;
6. **(Difficile)** $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$;

Solution.

1. $\exp: (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto \mathrm{e}^x$, $\ln: (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ sont les isomorphismes de groupes et $\exp^{-1} = \ln$.
2. Tout d'abord, l'app $(\mathbb{Z}/6\,\mathbb{Z}, +) \to (\mathbb{Z}/2\,\mathbb{Z}, +) \times (\mathbb{Z}/3\,\mathbb{Z}, +), a (\mathrm{mod}\, 6) \mapsto (a (\mathrm{mod}\, 2), a (\mathrm{mod}\, 3))$ est un morphisme de groupes. Par le thm des restes, cette app est bijective, donc c'est un isomorphisme de groupes.

   Remarque. $\mathbb{Z}/n\,\mathbb{Z} := (\mathbb{Z}/n\,\mathbb{Z}, +)$
3. Si $\mathrm{pgcd}(m, n) = 1$, alors l'app $\mathbb{Z}/m\,n\,\mathbb{Z} \to \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z}$ est un isomorphisme de groupes. Sinon, $G := \mathbb{Z}/m\,n\,\mathbb{Z} \ncong \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/n\,\mathbb{Z} =: H$ parce que $d := \mathrm{pgcd}(m, n)$, alors $G[d] = \{x \in \mathbb{Z}/m\,n\,\mathbb{Z} \mid d\,x \equiv 0 (\mathrm{mod}\, m\,n)\} = \{x \in \mathbb{Z}/m\,n\,\mathbb{Z} \mid x \equiv 0 (\mathrm{mod}\, m\,n/d)\}$, donc $\# G[d] = d$. Mais $H[d] = \{(x, y) \in G \mid (d\,x, d\,y) = (0 (\mathrm{mod}\, m), 0 (\mathrm{mod}\, n)) \in G\} = \{(x, y) \in G \mid x \equiv 0 (\mathrm{mod}\, m/d), y \equiv 0 (\mathrm{mod}\, n/d)\}$ dont le cardinal est d^2. $d > 1 \Longrightarrow d \neq d^2 \Longrightarrow G[d] \ncong H[d] \Longrightarrow G \ncong H$.
4. $(\mathbb{Z}/p\,\mathbb{Z})^\times \cong ((\mathbb{Z}/p\,\mathbb{Z}) \setminus \{0\}, \times)$ admet un générateur $a \in (\mathbb{Z}/p\,\mathbb{Z})^\times$ pour tout premier p. Pour cet a, l'app $\mathbb{Z}/(p-1)\,\mathbb{Z} \to (\mathbb{Z}/p\,\mathbb{Z})^\times, n (\mathrm{mod}\, p-1) \mapsto a^n$ est un isomorphisme de groupe (par définition de génerateur).
5. $G[3] = \{x \in \mathbb{R} \setminus \{0\} \mid x^3 = 1\} = \{1\}$. Pour autant, $H[3] = \{z \in \mathbb{C} \setminus \{0\} \mid z^3 = 1\}$ donc $\# H[3] = 3$. $G[3] \ncong H[3] \Longrightarrow G \ncong H$.

Exercice. (TD5 Ex3) Montrer que $H = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv b\ (\mathrm{mod}\, 2)\}$ est un sous-groupe de $\mathbb{Z}^2 = (\mathbb{Z}^2, +)$ et que l'application $f: \mathbb{Z}^2 \to H, (u, v) \mapsto u(2, 0) + v(1, 1) = (2\,u + v, v)$ est un isomorphisme de groupes.

Solution. Tout d'abord, l'élément neutre $(0, 0) \in H$. Ensuite, si $(a, b), (a', b') \in H$, alors $(a + a', b + b') \in H$ et $(-a, -b) \in H$. Donc $H \subseteq G$ est un sous-groupe. Pour montrer que f est un isom, il faut montrer que f est un morph de groupes: $f((u, v) + (u', v')) = f(u + u', v + v') = (2\,(u + u') + v + v', v + v') = (2\,u + v, v) + (2\,u' + v', v') = f(u, v) + f(u', v')$. Ensuite, $\operatorname{Ker}(f) = \{(u, v) \in \mathbb{Z}^2 \mid 2\,u + v = 0 \text{ et } v = 0\} = \{(0, 0) \in \mathbb{Z}^2\}$ et pour tout $(a, b) \in H$, on prend $v = b$ et $u = (b - a)/2$, alors $f(u, v) = (a, b) \in H$.

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

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?

Exercice. (Difficile?) Montrer: une app $f: \mathbb{Z}^2 \to \mathbb{Z}^2$ est un morphisme de groupes ss'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 le noyau de f. Quand est-ce que f est un isomorphisme de groupes?

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}.