Feuille de TD n° 1

Divisibilité, Congruences

8 septembre 2021

Pour commencer . . .

Exercice 1.

• Déterminer la division euclidienne de 154 par 12.
En déduire que 12 ne divise pas 154.

• On a $154 = 144 + 10 = 12 \times 12 + 10$. Le quotient est 12 et le reste 10. Comme le reste est non-nul, on sait alors que 12 ne divise pas 154.

Exercice 2.

• Simplifier modulo 15 : 7^2, 7×11, 7×13, et 7^3.
• Résoudre dans $\mathbb{Z}$ l'équation : $7n \equiv 2 \bmod (15)$.

• On a : $49 \equiv 4 \bmod (15)$, $77 \equiv 2 \bmod (15)$, $91 \equiv 1 \bmod (15)$, et $7^3 \equiv 4 \times 7 \equiv 13 \bmod (15)$.
• Soit n tel que $7n \equiv 2 \bmod (15)$.
En multipliant par 13, on obtient : $13 \times 2 \equiv 13 \times 7n \equiv 91n \equiv n \bmod (15)$.
Cela donne $n \equiv 26 \equiv 11 \bmod (15)$, c'est-à-dire $n = 11 + 15k$, $k \in \mathbb{Z}$.
Réciproquement, si $n \equiv 11 \bmod (15)$ alors on a $7n \equiv 77 \equiv 2 \bmod (15)$.
Donc l'ensemble des solutions de l'équation est $S = \{11 + 15k,\ k \in \mathbb{Z}\} = 11 + 15\mathbb{Z}$.

Exercice 3.

1. Calculer $\text{pgcd}(33, 28)$ avec l'algorithme d'Euclide.
2. Calculer $\text{pgcd}(12, 15)$ et $\text{ppcm}(12, 15)$. Calculer $\text{pgcd}(12, 15)\text{ppcm}(12, 15)$. Que trouve-t-on ?
3. Soit $n \in \mathbb{Z}$. Montrer que $\text{pgcd}(n^2, n^5 + 1) = 1$.

1. On a : $33 = 28 \cdot 1 + 5$, $28 = 5 \cdot 5 + 3$, $5 = 3 \cdot 1 + 2$.
$3 = 2 \cdot 1 + 1$, $2 = 1 \cdot 2 + 0$.
Donc, $\text{pgcd}(33, 28) = 1$.
2. On a : $15 = 12 \cdot 1 + 3$, $12 = 3 \cdot 4 + 0$. Donc, $\text{pgcd}(12, 15) = 3$.
On remarque que $60 = 12 \cdot 5 = 15 \cdot 4$ est un multiple commun de 12 et de 15.
Les multiples de 12 inférieurs à 60 sont : $12, 24, 36, 48$.
Les multiples de 15 inférieurs à 60 sont : $15, 30, 45$.
Ainsi, 60 est le plus petit multiple commun de 12 et 15 : $\text{ppcm}(12, 15) = 60$.
On obtient donc : $\text{pgcd}(12, 15)\text{ppcm}(12, 15) = 3 \cdot 60 = 180$.
On trouve : $12 \cdot 15 = 180 = \text{pgcd}(12, 15)\text{ppcm}(12, 15)$.
3. On a $(-n^3) \cdot n^2 + (n^5 + 1) = 1$. Le théorème de Bézout nous dit alors que $\text{pgcd}(n^2, n^5 + 1) = 1$.

Exercice 4.

1. Soit $n \in \mathbb{N}$. Démontrer que $11 \mid 3^{5n} + 5^{5n+1} + 4^{5n+2}$.
2. Déterminer le reste de la division euclidienne de 2^{65362} par 7.
3. Soit $n \in \mathbb{N}$. Montrer que 3 ne divise pas $n^2 + 1$.

1. On montre cela avec la congruence modulo 11.
• On a $3^2 \equiv -2 \bmod 11$, donc $3^4 \equiv (-2)^2 \equiv 4 \bmod 11$, puis $3^5 \equiv 4 \times 3 \equiv 1 \bmod 11$.
Comme $3^{5n} = (3^5)^n$, on obtient $3^{5n} \equiv 1^n \equiv 1 \bmod 11$.
• On a $5^2 \equiv 3 \bmod 11$, donc $5^4 \equiv 3^2 \equiv 9 \bmod 11$, puis $5^5 \equiv 9 \times 5 \equiv 45 \equiv 1 \bmod 11$.
Comme $5^{5n+1} = (5^5)^n \times 5$, on obtient $5^{5n+1} \equiv 1^n \times 5 \equiv 5 \bmod 11$.
• On a $4^2 \equiv 5 \bmod 11$, donc $4^4 \equiv 5^2 \equiv 3 \bmod 11$, puis $4^5 \equiv 3 \times 4 \equiv 1 \bmod 11$. Comme $4^{5n+2} = (4^5)^n \times 4^2$, on obtient $4^{5n+2} \equiv 1^n \times 16 \equiv 5 \bmod 11$.
Ainsi, on a $3^{5n} + 5^{5n+1} + 4^{5n+2} \equiv 1 + 5 + 5 \equiv 11 \equiv 0 \bmod 11$.
Donc 11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$.
2. On cherche à simplifier $2^{65362} \bmod (7)$ pour trouver le reste demandé.
On a $2^1 \equiv 2 \bmod 7$, $2^2 \equiv 4 \bmod 7$, $2^3 \equiv 1 \bmod 7$. Donc, d'après le cours, on a $(2^3)^n \equiv 1^n \bmod (7)$, pour tout $n \geq 0$.
La division euclidienne de 65362 par 3 donne : $65362 = 3 \times 21787 + 1$.
Donc $2^{65362} = (2^3)^{21787} \times 2$. Cela donne : $2^{65362} \equiv 1^{21787} \times 2 \equiv 2 \bmod 7$.
Comme $0 \leq 2 < 7$, on en déduit que le reste de la division euclidienne de 2^{65362} par 7 vaut 2.

3. On sait que 3 divise n^2+1 si et seulement si $n^2+1 \equiv 0 \bmod (3)$. Montrons que cela n'est jamais vrai.
   Soit $n \in \mathbb{Z}$. Le reste de la division euclidienne de n par 3 vaut 0 ou 1 ou 2. Cela donne 3 cas :
   -1$^{\text{er}}$ cas : Le reste vaut 0 : $n \equiv 0 \bmod 3$. Alors $n^2 \equiv 0 \bmod 3$ et donc $n^2+1 \equiv 1 \bmod 3$.
   -2$^{\text{ème}}$ cas : Le reste vaut 1 : $n \equiv 1 \bmod 3$. Alors $n^2 \equiv 1 \bmod 3$ et donc $n^2+1 \equiv 2 \bmod 3$.
   -3$^{\text{ème}}$ cas : Le reste vaut 2 : $n \equiv 2 \bmod 3$. Alors $n^2 \equiv 4 \equiv 1 \bmod 3$ et donc $n^2+1 \equiv 2 \bmod 3$.
   Donc dans tous les cas, n^2+1 n'est pas congru à 0 modulo 3. Donc 3 ne divise pas n^2+1.

Exercice 5.
• Montrer que pour tout $n \geq 0$, on a $10^n \equiv 1 \bmod (3)$.
• Démontrer la *règle de* 3 :
Soit $m \in \mathbb{N}$ dont l'écriture décimale est $m = \overline{a_r \dots a_0}$. Alors m est divisible par 3 si et seulement si la somme de ses chiffres $a_0 + \dots + a_r$ est divisible par 3.
• Démontrer la *règle de* 11 :
Soit $m \in \mathbb{N}$ dont l'écriture décimale est $m = \overline{a_r \dots a_0}$. Alors m est divisible par 11 si et seulement si la somme de ses chiffres $a_0 - a_1 + a_2 + \dots + (-1)^r a_r$ est divisible par 11.

• On a $10 \equiv 1 \bmod (3)$. D'après le cours, on a donc $10^n \equiv 1^n \equiv 1 \bmod (3)$, pour tout $n \geq 0$.
Autre preuve : Pour $n \geq 1$, $10^n - 1 = (10-1)\sum_{k=0}^{n-1} 10^k$, et $10 - 1 = 9$ est divisible par 3.
• L'entier m est divisible par 3 si et seulement si $m \equiv 0 \bmod (3)$.
On a $m = \sum_{k=0}^{r} a_k \cdot 10^k$, ce qui donne

$$m \equiv \sum_{k=0}^{r} a_k \bmod (3).$$

Donc m est divisible par 3 si et seulement si $a_0 + \dots + a_r$ est divisible par 3.
• L'entier m est divisible par 11 si et seulement si $m \equiv 0 \bmod (11)$.
On étudie $10^n \bmod (11)$. On a $10 \equiv -1 \bmod (11)$. D'après le cours, on a donc $10^n \equiv (-1)^n \bmod (11)$, pour tout $n \geq 0$.
Autre preuve : Pour $n \geq 1$, $10^n - (-1)^n = (10-(-1))\sum_{k=0}^{n-1} 10^k(-1)^{n-1-k}$, et $(10-(-1)) = 11$.
On a $m = \sum_{k=0}^{r} a_k \cdot 10^k$, ce qui donne donc :

$$m \equiv \sum_{k=0}^{r} a_k(-1)^k \bmod (11).$$

Donc m est divisible par 11 si et seulement si $a_0 + \dots + a_r$ est divisible par 11.

Exercice 6.
Soit $n \in \mathbb{Z}$. Déterminer $\text{pgcd}(n+2, n+5)$.
Déterminer les valeurs possibles de $\text{pgcd}(n+3, 2n^2-1)$.

• Soit $d = \text{pgcd}(n+2, n+5)$. Alors d est un diviseur de $n+2$ et $n+5$.
Donc, $d|(n+5)-(n+2) = 3$. On a donc $d = 1$ ou $d = 3$.
Réciproquement, si $n+2$ n'est pas divisible par 3, on a alors $d = 1$. Si $n+2$ est divisble par 3, alors $n+5$ aussi et $d = 3$.
On a $3 \mid n+2$ si et seulement si $n+2 = 3k$, $k \in \mathbb{Z}$.
On a donc $d = 3$ si $n = 3k-2$, $k \in \mathbb{Z}$, et $d = 1$ sinon.
• Soit $d = \text{pgcd}(n+3, 2n^2-1)$. Alors d est un diviseur de $n+3$ et $2n^2-1$.
Donc, $d|(2n^2-1) - 2n(n+3) = -6n-1$.
Donc, $d|(-6n-1) + 6(n+3) = 17$. On a donc $d = 1$ ou $d = 17$.
Réciproquement, si $n+3$ n'est pas divisible par 17, on a alors $d = 1$. Si $n+3$ est divisible par 17, alors $2n^2-1 = 2n(n+3) + (-6n-1) = 2n(n+3) + 17 - 6(n+3)$ est divisible par 17.
On a donc $d = 17$ si $n = 17k-3$, $k \in \mathbb{Z}$ et $d = 1$ sinon.

■ *Pour aller plus loin . . .*

Exercice 7. • Soit $n \geq 0$, tel que $n+2 \mid n^2+5$. Montrer que l'on a alors $n+2 \mid 9$.
• Trouver les $n \geq 0$ tels que $n+2 \mid n^2+5$.

• On a$n+2 \mid n+2$ et $n+2 \mid n^2+5$. Donc, $n+2 \mid n^2+5-n(n+2) = -2n+5$. Puis, $n+2 \mid -2n+5+2(n+2) = 9$. Donc, $n+2 \mid 9$.
• Si $n+2 \mid n^2+5$ on a $n+2 \mid 9$. Les diviseurs positifs de 9 sont $1, 3, 9$. Comme $n \geq 0$, on a donc $n = 1$ ou $n = 7$.
Réciproquement, si $n = 1$ on a $n+2 = 3$ et $n^2+5 = 6$, avec $3 \mid 6$. Si $n = 7$ on a $n+2 = 9$ et $n^2+5 = 54$, avec $9 \mid 54$.
Donc l'ensemble des solutions est $S = \{1, 7\}$.

Exercice 8. Soient $a, b \in \mathbb{N}$. Montrer que $7 \mid 10a+b$ si et seulement si $7 \mid a+5b$.
Est-ce que $7 \mid 1682$?

Supposons que $7 \mid 10a+b$. On a donc $10a+b \equiv 0 \bmod (7)$.

Donc, $0 \equiv 5(10a+b) \equiv 50a+5b \equiv a+5b \bmod (7)$.
Réciproquement, si $a+5b \equiv 0 \bmod (7)$, on a $0 \equiv 10(a+5b) \equiv 10a+50b \equiv 10a+b \bmod (7)$.
Le nombre 7 divise 1682 si et seulement si 7 divise $168+5*2=178$, si et seulement si 7 divise $17+40=57$. Comme $7 \nmid 57$, on en déduit que 7 ne divise pas 1682.

■ *Un peu de Géométrie . . .*

Exercice 9. Les ensembles suivants sont-ils des sous-espaces vectoriels de $\mathbb{R}^3$?

1. $F_1 = \{(x,y,z) \in \mathbb{R}^3 \mid x-4y=0\}$
2. $F_2 = \{(x,y,z) \in \mathbb{R}^3 \mid x-4y=1\}$
3. $F_3 = \{(x,y,z) \in \mathbb{R}^3 \mid x-4y \geq 0\}$
4. $F_4 = \{(x,y,z) \in \mathbb{R}^3 \mid x=y=z\}$
5. $F_5 = \{(x,y,z) \in \mathbb{R}^3 \mid xy=0\}$
6. $F_6 = \{(x,y,z) \in \mathbb{R}^3 \mid x \in \mathbb{N}\}$

---

1. Montrons que F_1 est un sous-espace vectoriel de $\mathbb{R}^3$. Soit $X=(x,y,z) \in F_1$, $X'=(x',y',z') \in F_1$ et $\lambda \in \mathbb{R}$:
   - $(0,0,0) \in F_1$;
   - $(x+x')-4(y+y')=(x-4y)+(x'-4y')=0$ donc $X+X' \in F_1$;
   - $\lambda x - 4\lambda y = \lambda(x-4y)=0$ donc $\lambda X \in F_1$.
2. Si $X, X' \in F_2$ alors $(x+x')-4(y+y')=2$ donc $X+X' \notin F_2$. Donc F_2 n'est pas un sous-espace vectoriel.
3. Si $X \in F_3$ vérifie $x-4y>0$ (par exemple : $X=(5,0,1)$), on a : $(-x)-4(-y)=-(x-4y)<0$ donc $-X \notin F_3$. Donc F_3 n'est pas un sous-espace vectoriel.
4. Montrons que F_4 est un sous-espace vectoriel de $\mathbb{R}^3$. Soit $X, X' \in F_4$ et $\lambda \in \mathbb{R}$:
   - $(0,0,0) \in F_4$;
   - $x+x'=y+y'=z+z'$ donc $X+X' \in F_4$;
   - $\lambda x = \lambda y = \lambda z$ donc $\lambda X \in F_4$.

   F_4 est donc un sous-espace vectoriel, c'est en fait la droite vectorielle $\mathbb{R}\begin{pmatrix}1\\1\\1\end{pmatrix}$.
5. On a : $(0,1,0) \in F_5$ et $(1,0,0) \in F_5$ mais $(0,1,0)+(1,0,0)=(1,1,0) \notin F_5$. Donc F_5 n'est pas un sous-espace vectoriel.
6. On a : $(1,0,0) \in F_6$ mais $\frac{1}{2}(1,0,0)=\left(\frac{1}{2},0,0\right) \notin F_6$. Donc F_6 n'est pas un sous-espace vectoriel.

Exercice 10. Montrer que les seuls sous-espaces vectoriels du $\mathbb{R}$-espace vectoriel $\mathbb{R}$ sont $\{0\}$ et $\mathbb{R}$.

Soit $F \subset \mathbb{R}$ un sous-espace vectoriel de $\mathbb{R}$. Supposons que $F \neq \{0\}$: il existe $x \neq 0$ tel que $x \in F$. Soit $y \in \mathbb{R}$, alors : $y = \frac{y}{x}.x \in F$. Donc $\mathbb{R} \subset F$, ce qui implique que $F=\mathbb{R}$.

Indications

Exercice 2

2 Trouver un k tel que $7k \equiv 1 \bmod (15)$.

Exercice 3

2 Chercher le plus petit multiple commun parmi les multiples de 12 et de 15.

Exercice 4

1. Regarder $(3^5)^n$,$(5^5)^n$,$(4^5)^n$ modulo 11.
2. Regarder les puissances de 2 modulo 7 :
   $2^0 \equiv ? \bmod 7$, $2^1 \equiv ? \bmod 7$, etc.
   Avec une division euclidienne bien choisie, en déduire une simplification de 2^{65362} modulo 7.
3. Regarder à quoi est congru n^2+1 modulo 3 selon que $n \equiv 0 \bmod 3$, $n \equiv 1 \bmod 3$, $n \equiv 2 \bmod 3$.

Exercice 5

2 Utiliser le lien entre divisibilité par n et congruence modulo n.
3 Commencer par calculer $10^n \bmod (11)$.

Exercice 6

1. Pour $d=\text{pgcd}(a,b)$, on a $d \mid a$ et $d \mid b$.

Exercice 8

1. Trouver k tel que $10k \equiv 1 \bmod (7)$.

Exercice 10

Si $x \in F$ alors $\lambda x \in F$ pour tout $\lambda \in \mathbb{R}$.