Mathématiques
Arithmétique

BackToBasics

10 juillet 2022

Table des matières

1 Cours **3**
1.1 Division euclidienne et PGCD 3
1.1.1 Division euclidienne 3
1.1.2 PGCD et nombres premiers entre eux 4
1.2 Théorème de Bézout 5
1.3 Nombres premiers 8
1.4 Congruences et Petit théorème de Fermat 9

2 Exercices **11**
2.1 Exercice 1 : Facteurs premiers et PGCD 11
2.2 Exercice 2 : Divisibilité 11
2.3 Exercice 3 : Reste de division euclidienne 11
2.4 Exercice 4 : Résolution d'équation 11

3 Correction **12**
3.1 Exercice 1 : Facteurs premiers et PGCD 12
3.2 Exercice 2 : Divisibilité 13
3.3 Exercice 3 : Reste de division euclidienne 14
3.4 Exercice 4 : Résolution d'équation 16

1 Cours

Dans ce cours, nous allons revoir tout ce qui concerne l'arithmétique. Si vous avez des questions sur n'importe quel point du cours, n'hésitez pas à poser votre question dans le salon dédié ou par messages privés sur Discord à **Swarwerth#2943**.

1.1 Division euclidienne et PGCD

1.1.1 Division euclidienne

Définition 1.1 : Divisibilité

Soient a et b deux éléments de l'ensemble $\mathbb{Z}$. On dit que a **divise** b s'il existe un $q \in \mathbb{Z}$ tel que

$$b = aq$$

On dit aussi que b **est divisible par** a ou que b **est multiple de** a.
On note $a|b$.

Propriété 1.2 :

$\forall (a, b, c) \in \mathbb{Z}^3$,

1. $a|a$, $\pm 1|a$ et $a|0$.
2. Si $a|b$ et $b|a$, alors $a = \pm b$.
3. Si $a|b$ et $b|c$, alors $a|c$.
4. Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$.
5. Si $a|b$ et $a|c$, alors $\forall (k, l) \in \mathbb{Z}^2, a|(kb + lc)$.

Théorème 1.3 : Division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe **un unique couple d'entiers** $(q, r) \in \mathbb{Z}^2$ tels que

$$a = bq + r \qquad \text{et } 0 \leq r < |b|$$

On dit que q est le **quotient** et r le **reste** de la division euclidienne de a par b.

La division euclidienne de 1208 par 23 est
$1208 = 23 \times 52 + 12$.

La division euclidienne de -1208 par 51 est
$-1208 = -24 \times 51 + 16$.

1.1.2 PGCD et nombres premiers entre eux

Définition 1.4 : PGCD et nombres premiers entre eux

Soit $(a, b) \in \mathbb{Z}^{*2}$,
- Le plus grand entier supérieur ou égal à 1 qui divise à la fois a et b s'appelle **plus grand diviseur commun** de a et b et se note $pgcd(a, b)$.
- Si $pgcd(a, b) = 1$, on dit que les nombres a et b sont **premiers** entre eux.

$pgcd(a, b) \iff a \wedge b$.

Propriété 1.5 : Lemme d'Euclide

Soit $(a, b) \in \mathbb{N}^{*2}$ et la division euclidienne $a = bq + r$.
On a alors,

$$pgcd(a, b) = pgcd(b, r)$$

1.2 Théorème de Bézout

Théorème 2.1 : Théorème de Bézout

Soient a et b deux entiers. Il existe $(x, y) \in \mathbb{Z}^2$ tel que

$$ax + by = pgcd(a, b)$$

On appelle alors x et y les **coefficients de Bézout**. Ils s'obtiennent en "remontant" l'algorithme d'Euclide. Ils ne sont pas uniques.

Utilisons l'algorithme d'Euclide pour déterminer le pgcd de 600 et 124.

$$\begin{aligned}
600 &= 124 \times 4 + 104 \\
124 &= 104 \times 1 + 20 \\
104 &= 20 \times 5 + 4 \\
20 &= 4 \times 5 + 0
\end{aligned}$$

Donc, $pgcd(600, 124) = 4$.

Remontons l'algorithme d'Euclide pour déterminer alors les coefficients de Bézout.

$$\begin{aligned}
4 &= 104 - 20 \times 5 \\
&= 104 - (124 - 104 \times 1) \times 5 \\
&= 104 \times 6 - 124 \times 5 \\
&= (600 - 124 \times 4) \times 6 - 124 \times 5 \\
&= 600 \times 6 - 124 \times 29
\end{aligned}$$

Propriété 2.2 :

Soit $(a, b, d) \in \mathbb{Z}^3$,

1. Si $d|a$ et $d|b$, alors $d|pgcd(a, b)$.
2. a et b sont **premiers entre eux** si et seulement s'il existe $(x, y) \in \mathbb{Z}^2$ tels que

$$ax + by = 1$$

Propriété 2.3 : Lemme de Gauss

Soit $(a, b, c) \in \mathbb{Z}^3$.
Si $a|bc$ et $pgcd(a, b) = 1$, alors $a|c$.

Propriété 2.4 : Résolution d'une équation

Soient $(a, b) \in \mathbb{Z}^{*2}$ et $c \in \mathbb{Z}$.

1. L'équation $ax + by = c$ a des **solution**s si et seulement si $pgcd(a, b)|c$.
2. Si $pgcd(a, b)|c$, alors il existe une **infinité de solutions entières**

$$(x, y) = (x_0 + \alpha k, y_0 + \beta k) \qquad \text{avec } (x_0, y_0, \alpha, \beta) \in \mathbb{Z}^4 \text{ et } k \text{ parcourant } \mathbb{Z}$$

La méthode pour résoudre une équation est la suivante :

1. Chercher s'il existe des solutions avec l'**algorithme d'Euclide**.
2. Trouver des solutions particulières avec le **théorème de Bézout**.
3. Rechercher toutes les solutions en utilisant le **lemme de Gauss**.

Soit l'équation (E) $203x - 84y = 14$ d'inconnues $(x, y) \in \mathbb{Z}^2$.
En utilisant l'algorithme d'Euclide, on a :

$$\begin{aligned}
203 &= 84 \times 2 + 35 \\
84 &= 35 \times 2 + 14 \\
35 &= 14 \times 2 + 7 \\
14 &= 7 \times 2 + 0
\end{aligned}$$

Donc, $pgcd(203, 84) = 7$.
Or, $7|14$, donc l'équation (E) admet des solutions.

En utilisant le théorème de Bézout, on a :

$$\begin{aligned}
7 &= 35 - 14 \times 2 \\
&= 35 - (84 - 35 \times 2) \times 2 \\
&= 35 - 84 \times 2 + 35 \times 4 \\
&= 35 \times 5 - 84 \times 2 \\
&= (203 - 84 \times 2) \times 5 - 84 \times 2 \\
&= 203 \times 5 - 84 \times 10 - 84 \times 2 \\
&= 203 \times 5 - 84 \times 12
\end{aligned}$$

$$\begin{aligned}
7 \times 2 &= 203 \times 10 - 84 \times 24 \\
14 &= 203 \times 10 - 84 \times 24
\end{aligned}$$

Donc, $x_0 = 10$ et $y_0 = 24$ sont des solutions particulières de (E).

D'après la première question, on a :

$$\begin{aligned} 203x - 84y = 203x_0 - 84y_0 &\iff 203(x - x_0) = 84(y - y_0) \\ &\iff 29(x - x_0) = 12(y - y_0) \end{aligned}$$

Utilisons l'algorithme d'Euclide pour déterminer si 29 et 12 sont premier entre eux ou non.

$$\begin{aligned} 29 &= 12 \times 2 + 5 \\ 12 &= 5 \times 2 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

Donc, $pgcd(29, 12) = 1$.
Ainsi, 12 et 29 sont premiers entre eux.

$$29(x - x_0) = 12(y - y_0)$$

Sachant que $(x - x_0) \in \mathbb{Z}$, on a par définition

$$29|12(y - y_0)$$

Or, 29 et 12 sont premiers entre eux.
Donc, d'après le lemme de Gauss, on a

$$29|y - y_0 \iff \exists k \in \mathbb{Z}, y - y_0 = 29k$$

Donc,

$$\begin{aligned} 29(x - x_0) &= 12(y - y_0) \\ 29(x - x_0) &= 12 \times 29k \\ x - x_0 &= 12k \end{aligned}$$

Ainsi, les solutions de (E) sont $(x, y) = (12k + 10, 29k + 24)$ avec $k \in \mathbb{Z}$.

1.3 Nombres premiers

Définition 3.1 : Nombre premier

Un nombre $p \in \mathbb{N}$ est dit **premier** si $p \geq 2$ et si ses **seuls diviseurs positifs** sont 1 et p.
Il existe une **infinité de nombres premiers**.

Propriété 3.2 :

Tout entier $n \geq 2$ admet au moins un diviseur premier.

Définition 3.3 : Crible d'Eratosthène

Soit $n \geq 2$. La méthode du **Crible d'Eratosthène** consiste à supprimer d'une table des entiers de 2 à n tous les multiples d'un entier.

On commence par rayer les multiples de 2, puis à chaque fois on raye les multiples du plus petit entier restant.

On peut s'arrêter lorsque le **carré du plus petit entier restant est supérieur au plus grand entier restant**. Enfin, on compte tous les entiers qui n'ont pas été rayés. Ce sont les nombres premiers inférieurs à n.

Propriété 3.4 : Lemme d'Euclide

Soient p un nombre premier et $(a, b) \in \mathbb{Z}^2$.
Si $p|ab$, alors $p|a$ ou $p|b$.

Théorème 3.5 :

Tout entier $n \geq 2$ admet une **décomposition unique en produit de nombres premiers**, c'est-à-dire qu'il existe des uniques nombres premiers $p_1 < p_2 < ... < p_r$ et $(\alpha_1, ..., \alpha_r) \in \mathbb{N}^{*r}$ tels que

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$$

1.4 Congruences et Petit théorème de Fermat

Définition 4.1 : Congruence

Soient $n \in \mathbb{N}^*$ et $(a,b) \in \mathbb{Z}^2$. On dit que a **est congru à** b modulo n et on note $a \equiv b[n]$ si b **divise** $b-a$. C'est-à-dire

$$a \equiv b[n] \iff \exists k \in \mathbb{Z}, a = b + kn$$

Propriété 4.2 :

Soit $n \in \mathbb{N}^*$. La relation **Congru modulo** n est une **relation d'équivalence**, c'est-à-dire :

1. Elle est **réflexive** : $\forall a \in \mathbb{Z}, a \equiv a[n]$.
2. Elle est **symétrique** : $\forall (a,b) \in \mathbb{Z}^2, a \equiv b[n] \iff b \equiv a[n]$.
3. Elle est **transitive** : $\forall (a,b,c) \in \mathbb{Z}^3$, si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$.

Propriété 4.3 :

Soient $n \in \mathbb{N}^* et (a,b,c,d) \in \mathbb{Z}^4$. Alors,

1. Si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a + c \equiv b + d[n]$.
2. Si $a \equiv b$ et $c \equiv d[n]$, alors $ac \equiv bd[n]$.
3. Si $a \equiv b[n]$, alors $\forall k \in \mathbb{N}, a^k \equiv b^k[n]$.

Théorème 4.4 : Petit théorème de Fermat

Soient p un nombre premier et $a \in \mathbb{Z}$.

$$a^p \equiv a[p]$$

Propriété 4.5 :

Soient p un nombre premier et $a \in \mathbb{Z}$.
Si p ne divise pas a, alors $a^{p-1} \equiv 1[p]$.

On a $39 = 5 \times 7 + 4$, donc 7 ne divise pas 39.
Sachant que 7 est premier, d'après le petit théorème de Fermat, on a :

$$39^6 \equiv 1[7]$$

Or, $129 = 6 \times 21 + 3$.
Donc,

$$\begin{aligned}
(39^6)^{21} &\equiv 1^{21}[7] \\
39^{6\times 21} \times 39^3 &\equiv 39^3[7] \\
39^{6\times 21+3} &\equiv 39^3[7] \\
39^{129} &\equiv 39^3[7]
\end{aligned}$$

Or, on a

$$\begin{aligned}
&39 \equiv 4[7] \\
&39 \equiv -3[7]
\end{aligned}$$

$$\begin{aligned}
&39^2 \equiv (-3)^2[7] \\
&39^2 \equiv 9[7] \\
&39^2 \equiv 2[7]
\end{aligned}$$

On a alors

$$\begin{aligned}
39^3 &\equiv 39^2 \times 39[7] \\
&\equiv 2 \times -3[7] \\
&\equiv -6[7] \\
&\equiv 1[7]
\end{aligned}$$

Or, $0 \leq 1 < 7$.
Donc, le reste de la division euclidienne de 39^{129} par 7 est égal à 1.

2 Exercices

Nous avons essayé de mettre l'ensemble des connaissance à savoir pour les rattrapages au niveau du chapitre sur les suites. Évidemment, vous avez le droit de relire le cours ou de poser des questions. Ces exercices permettront de pointer les lacunes que vous pourriez avoir.

2.1 Exercice 1 : Facteurs premiers et PGCD

1. Décomposer en facteurs premiers les nombres $A = 12825$ et $B = 9240$. En déduire le PGCD de A et B.
2. Déterminer le PGCD de 2244 et 1089 et déterminer l'idendité de Bézout correspondante.

2.2 Exercice 2 : Divisibilité

1. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.
2. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{n+3} - 5 \times 4^{4n}$ est divisible par 11.

2.3 Exercice 3 : Reste de division euclidienne

1. Calculer le reste dans la division euclidienne de 529^{326} par 17.
2. Calculer le reste dans la division euclidienne de 288^{288} par 29.

2.4 Exercice 4 : Résolution d'équation

1. (a) À l'aide de l'algorithme d'Euclide, calculer le PGCD de 237 et 156 et donner un couple de coefficients de Bézout associés.
   (b) Résoudre dans $\mathbb{Z}^2$ l'équation $237x + 156y = 3$.
2. (a) À l'aide de l'algorithme d'Euclide, calculer le PGCD de 972 et 504 et donner un couple de coefficients de Bézout associés.
   (b) Résoudre dans $\mathbb{Z}^2$ l'équation $972x + 504y = 72$.

3 Correction

Voici la correction des exercices du PDF. Nous vous invitons à faire les exercices avant de lire la correction. Pour toute question, merci de vous rediriger vers le cours et les professeurs présents.

3.1 Exercice 1 : Facteurs premiers et PGCD

1. Décomposer en facteurs premiers les nombres $A = 12825$ et $B = 9240$. En déduire le PGCD de A et B.

$A = 12825 = 19 \times 5^2 \times 3^3$ et $B = 9240 = 11 \times 7 \times 5 \times 3 \times 2^3$
On a alors

$$pgcd(A, B) = 19^0 \times 11^0 \times 7^0 \times 5^1 \times 3^1 \times 2^0 = 15$$

2. Déterminer le PGCD de 2244 et 1089 et déterminer l'idendité de Bézout correspondante.

En utilisant l'algorithme d'Euclide, on a

$$\begin{aligned}
2244 &= 1089 \times 2 + 66 \\
1089 &= 66 \times 16 + 33 \\
66 &= 33 \times 2 + 0
\end{aligned}$$

Donc, $pgcd(2244, 1089) = 33$.

En remontant l'algorithme d'Euclide, on a

$$\begin{aligned}
33 &= 1089 - 66 \times 16 \\
&= 1089 - (2244 - 1089 \times 2) \times 16 \\
&= 1089 \times 33 - 2244 \times 16
\end{aligned}$$

3.2 Exercice 2 : Divisibilité

1. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

Montrons que $3^{2n+1} + 2^{n+2} \equiv 0[7]$.
On a $3^{2n+1} = (3^2)^n \times 3^1 = 9^n \times 3$ et $2^{n+2} = 2^n \times 2^2 = 2^n \times 4$.
Ainsi,

$$3^{2n+1} + 2^{n+2} = 9^n \times 3 + 2^n \times 4$$

Pour $n = 0$,
$9^0 \times 3 + 2^0 \times 4 = 7$ et $7 \equiv 0[7]$.

Pour $n \neq 0$,
$9 \equiv 2[7]$, donc $9^n \equiv 2^n[7]$.

$$\begin{aligned} 3^{2n+1} + 2^{n+2} &\equiv 9^n \times 3 + 2^n \times 4[7] \\ &\equiv 2^n \times 3 + 2^n \times 4[7] \\ &\equiv 2^n(3+4)[7] \\ &\equiv 2^n \times 7[7] \\ &\equiv 0[7] \end{aligned}$$

Donc, $\forall n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

2. Montrer (sans récurrence) que pour tout $n \in \mathbb{N}$, $3^{n+3} - 5 \times 4^{4n}$ est divisible par 11.

Montrons que $3^{n+3} - 5 \times 4^{4n} \equiv 0[11]$.

$$\begin{aligned} 3^{n+3} &\equiv 3^n \times 27[11] \\ &\equiv 3^n \times 5[11] \end{aligned}$$

$$\begin{aligned} 4^{4n} &\equiv ((4^2)^2)^n[11] \\ &\equiv (16^2)^n[11] \\ &\equiv (5^2)^n[11] \\ &\equiv 25^n[11] \\ &\equiv 3^n[11] \end{aligned}$$

$$\begin{aligned} 3^{n+3} - 5 \times 4^{4n} &\equiv 3^n \times 5 - 5 \times 4^{4n}[11] \\ &\equiv 0[11] \end{aligned}$$

Donc, $\forall n \in \mathbb{N}$, $3^{n+3} - 5 \times 4^{4n}$ est divisible par 11.

3.3 Exercice 3 : Reste de division euclidienne

1. Calculer le reste dans la division euclidienne de 529^{326} par 17.

On a $529 = 31 \times 17 + 2$, donc 17 ne divise pas 529.
Sachant que 17 est premier, d'après le petit théorème de Fermat, on a

$$529^{16} \equiv 1[17]$$

Or, $326 = 16 \times 20 + 6$.
Donc,

$$\begin{aligned}
(529^{16})^{20} &\equiv 1^{20}[17] \\
529^{16\times 20} \times 529^{6} &\equiv 1 \times 529^{6}[17] \\
529^{326} &\equiv 529^{6}[17]
\end{aligned}$$

Or, $529 \equiv 2[17]$

$$\begin{aligned}
529^{6} &\equiv 2^{6}[17] \\
&\equiv 64[17] \\
&\equiv 13[17]
\end{aligned}$$

Or, $0 \leq 13 < 17$.
Donc, le reste de la division euclidienne de 529^{326} par 17 est égal à 13.

2. Calculer le reste dans la division euclidienne de 288^{288} par 29.

On a $288 = 9 \times 29 + 27$, donc 29 ne divise pas 288.
Sachant que 29 est premier, d'après le petit théorème de Fermat, on a

$$288^{28} \equiv 1[29]$$

Or, $288 = 28 \times 10 + 8$.
Donc,

$$\begin{aligned}(288^{28})^{10} &\equiv 1^{10}[29]\\ 288^{28\times 10} \times 288^{8} &\equiv 1 \times 288^{8}[29]\\ 288^{288} &\equiv \times 288^{8}[29]\end{aligned}$$

Or, on a

$$288 \equiv 27[29]$$
$$288 \equiv -2[29]$$

$$288^2 \equiv 4[29]$$
$$288^4 \equiv 16[29]$$
$$288^4 \equiv -13[29]$$

$$288^8 \equiv 69[29]$$
$$288^8 \equiv 24[29]$$

Or, $0 \leq 24 < 29$.
Donc, le reste de la division euclidienne de 288^{288} par 29 est 24.

3.4 Exercice 4 : Résolution d'équation

1. (a) À l'aide de l'algorithme d'Euclide, déterminer une solution particulière de l'équation $237x + 156y = 3$.

En utilisant l'algorithme d'Euclide, on a

$$\begin{aligned} 237 &= 156 \times 1 + 81 \\ 156 &= 81 \times 1 + 75 \\ 81 &= 75 \times 1 + 6 \\ 75 &= 6 \times 12 + 3 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

Donc, $pgcd(237, 156) = 3$.
Avec le théorème de Bézout, on a

$$\begin{aligned} 3 &= 75 - 6 \times 12 \\ &= 75 - (81 - 75) \times 12 \\ &= 75 \times 13 - 81 \times 12 \\ &= (156 - 81) \times 13 - 81 \times 12 \\ &= 156 \times 13 - 81 \times 25 \\ &= 156 \times 13 - (237 - 156) \times 25 \\ &= 156 \times 38 - 237 \times 25 \end{aligned}$$

Ainsi, une solution particulière existe avec $(x_0, y_0) = (-25, 38)$.

(b) En utilisant le théorème de Gauss, déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $237x+156y = 3$.

$$\begin{aligned} 237x + 156y = 237x_0 + 156y_0 &\iff 237(x - x_0) = -156(y - y_0) \\ &\iff 79(x - x_0) = -52(y - y_0) \end{aligned}$$

Donc, $79 | -52(y - y_0)$.
Or, $pgcd(79, 52) = 1$.
Ainsi, en utilisant le lemme de Gauss, on a

$$79 | y - y_0 \iff \exists k \in \mathbb{Z}, y - y_0 = 79k$$

Ainsi,

$$\begin{aligned} 79(x - x_0) &= -52 \times 79k \\ x - x_0 &= -52k \end{aligned}$$

Donc, $(x, y) = (-52k - 25, 79k + 38)$.

2. (a) À l'aide de l'algorithme d'Euclide, déterminer une solution particulière de l'équation $329x - 217y = 21$.

En utilisant l'algorithme d'Euclide, on a

$$\begin{aligned} 329 &= 217 \times 1 + 112 \\ 217 &= 112 \times 1 + 105 \\ 112 &= 105 \times 1 + 7 \\ 105 &= 7 \times 15 + 0 \end{aligned}$$

Donc, $pgcd(329, 217) = 15$.
Avec le théorème de Bézout, on a

$$\begin{aligned} 7 &= 112 - 105 \\ &= 112 - (217 - 112) \\ &= 112 \times 2 - 217 \\ &= (329 - 217) \times 2 - 217 \\ &= 329 \times 2 - 217 \times 3 \\ 7 \times 3 &= 3(329 \times 2 - 217 \times 3) \\ 21 &= 329 \times 6 - 217 \times 9 \end{aligned}$$

Ainsi, une solution particulière existe avec $(x_0, y_0) = (6, 9)$.

(b) En utilisant le théorème de Gauss, déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $329x - 217y = 21$.

$$\begin{aligned} 329x - 217y = 329x_0 - 217y_0 &\iff 329(x - x_0) = 217(y - y_0) \\ &\iff 74(x - x_0) = 31(y - y_0) \end{aligned}$$

Donc, $74|31(y - y_0)$.

$$\begin{aligned} 74 &= 31 \times 2 + 12 \\ 31 &= 12 \times 2 + 7 \\ 12 &= 7 \times 1 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

Donc, $pgcd(74, 31) + 1$.
Ainsi, en utilisant le lemme de Gauss, on a

$$74|y - y_0 \iff \exists k \in \mathbb{Z}, y - y_0 = 74k$$

Ainsi,

$$\begin{aligned} 74(x - x_0) &= 31 \times 74k \\ x - x_0 &= 31k \end{aligned}$$

Donc, $(x, y) = (31k + 6, 74k + 9)$.