Exercices : 6, 7, 14, 9, 10 (a,b)
16.

Exercice 6 Pgcd.

Pgcd(a,b) = d $\exists u, v$

tq $au + bv = d$. Bézout.

⚠ il n'y a pas unicité.

Théorème d'Euclide

pgcd(a,b)

$a = bq + r$ (division euclidienne de a par b)

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

Exercice 6 :

1) $pgcd(230, 126) = D$

$230 = 126 \times 1 + 104$

$D = pgcd(126, 104)$

(Thm d'Euclide)

$126 = 104 + 22$

Donc $D = pgcd(104, 22)$

$104 = 4 \times 22 + 16$)

$D = pgcd(22, 16)$

$22 = 16 + 6$

$D = pgcd(16, 6)$

$$16 = 6 \times 2 + 4$$

$D = pgcd(6, 4)$

$6 = 4 + 2$ PGCD

$D = pgcd(4, 2) = 2$

$4 = 2 \times 2$

$pgcd(230, 126) = 2$

On cherche $u, v \in \mathbb{Z}$

tq $u230 + v126 = 2$

de l'identité de Euclide.

$$2 = 6 - 4$$
$$= 6 - (16 - 6\times 2)$$
$$2 = 6\times 3 - 16$$
$$2 = (22 - 16)\times 3 - 16$$
$$2 = 22\times 3 - 16\times 4$$
$$= 22\times 3 - (104 - 4\times 22)4$$
$$2 = 22\times 20 - 104\times 4$$
$$= 22\times 20 - (126 - 22)\times 4$$
$$= 22\times 44 - 126\times 4$$
$$2 = (126 - 104)\times 24 - 126\times 4$$
$$= 126\times 20 - 104\times 24$$
$$= 126\times 20 - (230 - 126)\times 24$$

$$\boxed{2 = 126\times 44 - 230\times 24}$$

L'identité de Bézout

2) $pgcd(a, b)$

Si $(m \mid a$ et $m \mid b) \Leftrightarrow m \mid pgcd(a,b)$

Si $(m \mid a$ et $m \mid b$ et $m \mid c)$

$\Leftrightarrow (m \mid pgcd(a,b)$ et $m \mid c)$

$\Leftrightarrow m \mid pgcd(c, pgcd(a,b))$.

On peut changer les rôles de a, b et c.

$pgcd(c, pgcd(a,b))$

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

$= pgcd(a, b, c)$

3) a) pgcd(390, 720, 450)

pgcd(720, 390)

= 10 × (pgcd(72, 39))

72 = 39 + 33

D = pgcd(39, 33) = pgcd(33, 6)

39 = 33 + 6 = 3

Donc pgcd(720, 390) = 30

Il faut calculer pgcd(30, 450)

= 10 × pgcd(3, 45)

= 10 × 3 = 30

Pgcd(390, 720, 450) = 30

b) $pgcd(180, 606) = D$

$606 = 180 \times 3 + 66$

$180 \times 3 = 540$

$D = pgcd(180, 66)$

$180 = 2 \times 66 + 48$

132

$D = pgcd(66, 48)$

$66 = 48 + 18$

$D = pgcd(48, 18)$

$48 = 18 \times 2 + 12$

$D = pgcd(18, 12) = 6$

Pgcd(180, 606) = 6

Pgcd(6, 750) = 6

750 = 125 × 6

Donc Pgcd(180, 606, 750) = 6

Exercice 7

$a \in \mathbb{N}^*$

a) On cherche m et n

$$\begin{cases} \text{Pgcd}(m, n) = 18 \\ m + n = 360 \end{cases}$$

Donc $m = 18a$

et $n = 18b$.

On Pgcd$(m, n) = 18$

Et en plus pgcd(a,b) = 1

(a et b sont premiers entre eux)

$M + m = 360$

$18(a+b) = 360$

$36 = 18 \times 2$

donc il faut trouver

a et b tq

$$\begin{cases} pgcd(a,b) = 1 \\ a+b = 20 \end{cases}$$

Trouver $a, b \in \mathbb{N}^*$

(19, 1)

(a, b)

(18, 2)

(17, 3)

(16, 4)

(15, 5)

(14, 6)

(13, 7)

(12, 8)

(11, 9)

(10, 10)

(9, 11)

(7, 13)

(3, 17)

(1, 19)

8 couples !

Le résultat est donc de 8 couples (il faut multiples par 19).

b) $\begin{cases} pgcd(m,n) = 18 \\ mn = 6480 \end{cases}$

On a $\begin{cases} m = 18a \\ n = 18b \end{cases}$ $pgcd(a,b) = 1$

$mn = (18)^2 ab = 6480$

$= (18)^2 \times 20$

Donc on cherche $a, b \in \mathbb{N}^*$

tq $\begin{cases} pgcd(a,b) = 1 \\ ab = 2 \end{cases}$

$(1,20)$, $(4,5)$, $(5,2)$, $(20,1)$

(ce sont les couples (a,b))

La solution est l'ensemble

$\{(18, 18\times 20), (18\times 4, 18\times 5),$

$(18\times5, 18\times4), (17\times20, 18)$.

Exercice 4 :

1) Facteurs premiers

$12 = 4\times3 = 2^2\times3$

2) Diviseurs de 12

$\{1, 2, 3, 4, 6, 12\}$

Exercice 9

a) On cherche $(a, b)\in\mathbb{Z}\times\mathbb{Z}$

$18a + 5b = 11$

Le but est de trouver une solution.

$pgcd(18, 5) = 1$

$18 = 5 \times 3 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2$

$1 = 3 - (5 - 3)$

$1 = 3 \times 2 - 5$

($pgcd(5, 3) = 1$)

$1 = (18 - 5\times 3)\times 2 - 5$

$1 = 18\times 2 - 5\times 7$

Décomposition de Bezout.

Donc

$11 = 18\times 22 - 5\times 77$

On a une solution particulière au problème

$(22, -77)$.

On cherche l'ensemble des solutions $18a + 5b = 11$

$\Leftrightarrow 18a + 5b = 18 \times 22 - 5 \times 77$

$\Leftrightarrow \boxed{18(a-22) = 5(-b-77)}$

Mais $pgcd(18, 5) = 1$

$\exists k \in \mathbb{Z} \quad a - 22 = 5k$.

$(a - 22 \mid 5)$

Et $-b - 77 = 18k$.

L'ensemble des solutions est

$\boxed{\{(22 + 5k, -18k - 77),\ k \in \mathbb{Z}\}}$

$a - 22 = 55$

$18 \times 55 = (-5 - 7 + 7) 5$

b) On cherche $a, b \in \mathbb{Z}$

$39a - 12b = 121$

Pgcd (39, 12)

$39 = 3 \times 12 + 3$

$39 - 3 \times 12 = 3$

Donc $3 \mid 39a$

et $3 \mid 12b$

Mais 3 ne divise pas 121

Donc il n'y a pas de solution

$14a - 21b = 49$

$\Leftrightarrow 2a - 3b = 7$

$Pgcd(2, 3) = 1$

$1 = 2 \times 2 - 3$ (Bézout)

On a une solution particulière

$7 = 2 \times 14 - 3 \times 7$

Donc $(14, 7)$ est une solution particulière.

$2a - 3b = 2 \times 14 - 3 \times 7$

$2(a - 14) = 3(b - 7)$

Puisque $Pgcd(2, 3) = 1$

$\exists k \in \mathbb{Z}$, $a - 14 = 3 \times k$

donc $b - 7 = 2 \times k$

L'ensemble des solutions est $\{(14+3k, 7+2k),\ k \in \mathbb{Z}\}$

Exercice 10 (a b) :

a) $\begin{cases} n \equiv 1 \ [20] \\ n \equiv 3 \ [7] \end{cases}$

$\rightsquigarrow$ Pgcd (20, 7)

(décomposition de Bézout)

Pgcd (20, 7) = 1

$3 \times 7 - 20 = 1$

(Décomposition de Bézout)

On cherche une solution particulière.

$1 = -20 + 3 \times 7$

$M_0 = (-20) \times 3 + (3 \times 7) \times 1$

$M_0 \equiv 3 \times 7 \quad [20]$

$\equiv 1 + 20 \quad [20]$

$M_0 \equiv 1 \quad [10]$

$M_0 \equiv (-20) \times 3 \quad [7]$

$\equiv (1 - 3 \times 7) \times 3 \quad [7]$

$M_0 \equiv 3 \quad [7]$

M_0 est bien une solution particulière

Si $\begin{cases} n \equiv 1 \ [20] \\ n \equiv 3 \ [7] \end{cases}$

$\Leftrightarrow \begin{cases} n \equiv n_0 \ [20] \\ n \equiv n_0 \ [7] \end{cases}$

$20 \mid n - n_0$

$7 \mid n - n_0$

$\text{Pgcd}(7, 20) = 1$

Donc $140 \mid n - n_0$

$\exists k \in \mathbb{Z}, \quad n - n_0 = 140k$

L'ensemble des solutions est

$\{n = n_0 + 140k, \ k \in \mathbb{Z}\}$.

b) $\begin{cases} n \equiv 13 \ [15] \\ n \equiv 6 \ [10] \end{cases}$

⚠ $\text{Pgcd}(15,10) = 5 \neq 1$

Ça implique qu'il existe a, b tq $n = 13 + a\,15$

$n = 6 + b\,10$

$n \equiv 13 \ [5] \equiv 3 \ [5]$

$n \equiv 6 \ [5] \equiv 1 \ [5]$

C'est impossible, il n'y a pas de solutions.

Exercice 16 et 17 :

16) $\forall n, \ n^5 - n \equiv 0 \ [15]$

15 = 3x 5

$n^5 - n \equiv 0 \ [3]$

or $n^5 - n \equiv 0 \ [5]$

Modulo 3

- $n \equiv 0 \ [3] \Rightarrow n^5 \equiv 0 \ [3]$

  $n^5 \equiv n \ [3]$

- $n \equiv 1 \ [3] \Rightarrow n^5 \equiv 1 \ [3]$

  $n^5 \equiv n \ [3]$

- $n \equiv 2 \ [3] \Rightarrow n \equiv -1 \ [3]$

  $n^5 \equiv -1 \ [3]$

  $n^5 \equiv n \ [3]$

Modulo 5

$n \equiv 0 \ [5]$, $n^5 \equiv 0 \ [5]$

$n \equiv 1 \ [5]$, $n^5 \equiv 1 \ [5]$

$n \equiv 2 \ [5]$, $n^5 \equiv 2^5$

$\equiv 32 \ [5]$

$\equiv 2 \ [5]$

$n \equiv 3 \ [5]$

$\Rightarrow n \equiv -2 \ [5] \Rightarrow$

$n^5 \equiv -2 \ [5]$

$n \equiv 4 \ [5]$, $n \equiv -1 \ [5]$

$n^5 \equiv -1 \ [5]$

Όμως $n^5 - n \equiv 0 \ [5]$.

Autre méthode

$$n^5 - n = n(n^4 - 1)$$

$$= n(n-1)(n+1)(n^2+1)$$

$$= n(n^2-1)(n^2+1)$$

$n^5 - n$ est divisible par 3 et 5.

- C'est divisible par 3 car $(n-1)n(n+1)$ est le produit de 3 entiers consécutifs

$$\forall n < 3 \mid (n-1)n(n+1)$$

- Si $n \geq 5$ $\mid (n-1)n(n+1)$,

on a gagné.

Si $5 \mid (n-1)n(n+1)$

alors on peut vérifier

que $n \equiv 2 [5]$ ou

bien $n \equiv 3 [5]$

Donc ce cas on a

$n^2 + 1 \equiv 0 [5]$

Donc $5 \mid n^5 - n$.

Exercice 17

$\forall p$ premier, $p \geq 5$
alors $p^2 \equiv 1 \ [24]$

$p^2 - 1 = (p+1)(p-1)$

$24 = 8 \times 3$

$p^2 - 1 \equiv 0 \ [8]$

et $p^2 - 1 \equiv 0 \ [3]$

Car $pgcd(8,3) = 1$.

Modulo 8

---

p est premier :
p est impair

Car $p \geq 5$

$p-1$ pair

$p+1$ aussi

$2 \times b = 4 \times a$

$p-1$ et $p+1$ sont

2 entiers pairs consécutifs

Donc l'un des deux

est multiple de 4.

et l'autre de 2

Donc $(p-1)(p+1) \equiv 0 \ [8]$

Modulo 3

$p-1$, p , $p+1$

sont 3 entiers consécutifs

Donc un des 3 nombres $\equiv 0 \ [3]$

$p \not\equiv 0 \ [3]$

Car p est premier et $p \geq 5$

Donc $p-1 \equiv 0 \ [3]$

ou bien $p+1 \equiv 0 \ [3]$

Donc $p^2-1 \equiv 0 \ [3]$

Puisque $pgcd(8,3) = 1$

$p^2 - 1 \equiv 0 \ [24]$.

Esc. 22