Maths XP CS $n°4$ 5 Mars 2025 **Thiaude P.**
Durée : 1h Calculatrice interdite

Info : les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés nombres de Mersenne.
(image : source wikipedia)

Le moine français Marin **Mersenne** (1588-1648)

Exercice 1 [6 points]

Préambule
On souhaite déterminer le plus petit diviseur de $2^{33} - 1$ strictement plus grand que 1.

1. $2^{33} - 1$ est-il divisible par 2 ?

2. Justifier que : $2^{33} - 1 \equiv 1\ [3]$. Le nombre $2^{33} - 1$ est-il divisible par 3 ?

3. $2^{33} - 1$ est-il divisible par 4 ?

4. $2^{33} - 1$ est-il divisible par 5 ?

5. $2^{33} - 1$ est-il divisible par 6 ?

6. $2^{33} - 1$ est-il divisible par 7 ?

Répondre à la problématique évoquée dans le préambule.

Exercice 2 [4 points]

1. Montrer que : $6^5 \equiv -1\ [11]$.

2. Démontrer que : $55 | 6^{70} - 1$.

Exercice 3 [10 points] (d'après BAC)

On considère l'équation (E) d'inconnue $(x, y) \in \mathbb{Z}^2$: $17x - 40y = 1$.

1. À l'aide de l'algorithme d'Euclide déterminer $\mathrm{PGCD}(17, 40)$.

2. En déduire une solution particulière (x_0, y_0) de (E).

3. Résoudre (E).

4. Montrer que 17 admet un unique inverse modulo 40 strictement compris entre 35 et 75, en donner la valeur.

BONUS [2 points]

Pour $a \in \mathbb{Z}$, déterminer $\mathrm{PGCD}(3a + 5, 7a + 6)$.

Corrigé

Exercice 1

On cherche à déterminer le plus petit diviseur de $2^{33}-1$ strictement supérieur à 1.

1. **$2^{33}-1$ est-il divisible par 2 ?**
   Raisonnons modulo 2 : $2^{33}-1 \equiv 0^{33}-1 \equiv -1 \equiv -1+2 \equiv 1\ [2]$.
   On a $2^{33}-1 \equiv 1\ [2]$ avec $0 \leqslant 1 < 2$ donc le reste modulo 2 de $2^{33}-1$ est 1 :
   ce n'est pas 0 donc **$2^{33}-1$ n'est pas divisible par 2**.

2. **Justifier que : $2^{33}-1 \equiv 1\ [3]$. Le nombre $2^{33}-1$ est-il divisible par 3 ?**
   Raisonnons modulo 3 :
   $2^{33}-1 \equiv (2-3)^{33}-1 \equiv (-1)^{33}-1 \equiv -1-1 \equiv -2+3 \equiv 1\ [3]$.
   On a $2^{33}-1 \equiv 1\ [3]$ avec $0 \leqslant 1 < 3$ donc le reste modulo 3 de $2^{33}-1$ est 1 :
   ce n'est pas 0 donc **$2^{33}-1$ n'est pas divisible par 3**.

3. **$2^{33}-1$ est-il divisible par 4 ?**
   Raisonnons modulo 4 :
   $2^3 = 8 \equiv 8-2\times 4 \equiv 0\ [4]$
   $2^{33}-1 = (2^3)^{11}-1 \equiv 0^{11}-1 \equiv -1 \equiv -1+4 \equiv 3\ [4]$
   0n a $2^{33}-1 \equiv 3\ [4]$ avec $0 \leqslant 3 < 4$ donc le reste modulo 4 de $2^{33}-1$ est 3 :
   ce n'est pas 0 donc **$2^{33}-1$ n'est pas divisible par 4**.

4. **$2^{33}-1$ est-il divisible par 5 ?**
   Raisonnons modulo 5 :
   $2^2 = 4 \equiv 4-5 \equiv -1\ [5]$
   $2^{33}-1 = 2^{2\times 16+1}-1 = (2^2)^{16}\times 2^1 - 1 \equiv (-1)^{16}\times 2 - 1 \equiv 1\times 2-1 \equiv 1\ [5]$
   On a $2^{33}-1 \equiv 1\ [5]$ avec $0 \leqslant 1 < 5$ donc le reste modulo 5 de $2^{33}-1$ est 1 : ce n'est pas 0 donc **$2^{33}-1$ n'est pas divisible par 5**.

5. **$2^{33}-1$ est-il divisible par 6 ?**
   Supposons que $6|2^{33}-1$: il existe $k \in \mathbb{N}$ tel que $2^{33}-1 = 6k = 2\times 3k$.
   Il existe $k' \in \mathbb{N}$ tel que $2^{33}-1 = 2k'$, à savoir $k' = 3k$, donc $2^{33}-1$ est divisible par 2 ce qui est FAUX d'après la question **1.**, donc il faut rejeter la supposition par conséquent **$2^{33}-1$ n'est pas divisible par 6**.

6. **$2^{33}-1$ est-il divisible par 7 ?**
   Raisonnons modulo 7 :
   $2^3 = 8 \equiv 8-7 \equiv 1\ [7]$
   $2^{33}-1 = (2^3)^{11}-1 = 8^{11}-1 \equiv 1^{11}-1 \equiv 1-1 \equiv 0\ [7]$
   On a : $2^{33}-1 \equiv 0\ [7]$ donc : **$7|2^{33}-1$**.

   Le plus petit entier naturel non nul qui divise $2^{33}-1$ est donc 7.

Exercice 2

1. **Montrer que : $6^5 \equiv -1\ [11]$.**
   $6^2 = 36 \equiv 36 - 3 \times 11 \equiv 3\ [11]$
   $6^5 = (6^2)^2 \times 6 \equiv 3^2 \times 6 \equiv 9 \times 6 \equiv 54 \equiv 54 - 5 \times 11 \equiv 54 - 55 \equiv -1\ [11]$,
   donc on a bien : $\mathbf{6^5 \equiv -1\ [11]}$.

2. **Démontrer que : $55|6^{70} - 1$**
   • **montrons que $5|6^{70} - 1$**
   Raisonnons modulo 5.
   On a : $6 \equiv 6 - 5 \equiv 1\ [5]$, donc : $6^{70} - 1 \equiv 1^{70} - 1 \equiv 1 - 1 \equiv 0\ [5]$
   Résumons : $6^{70} - 1 \equiv 0\ [5]$, donc : $\mathbf{5|6^{70} - 1}$.

   • **montrons que : $11|6^{70} - 1$**
   Raisonnons modulo 11.
   On a : $6^{70} - 1 = (6^5)^{14} - 1 \equiv (-1)^{14} - 1 \equiv 1 - 1 \equiv 0\ [11]$
   On a : $6^{70} - 1 \equiv 0\ [11]$, donc : $\mathbf{11|6^{70} - 1}$.

   • **montrons que $55|6^{70} - 1$**
   $\mathrm{PGCD}(5, 11) = \mathrm{PGCD}(11 - 2 \times 5, 11) = \mathrm{PGCD}(1, 11) = 1$ donc 5 et 11 sont premiers entre eux ; on a : $5|6^{70} - 1$ et $11|6^{70} - 1$ avec 5 et 11 premiers entre eux donc d'après le corollaire du théorème de GAUSS on en déduit : $5 \times 11|6^{70} - 1$, c'est-à-dire : $\mathbf{55|6^{70} - 1}$.

Exercice 3

On considère l'équation (E) d'inconnue $(x, y) \in \mathbb{Z}^2$: $17x - 40y = 1$.

1. **À l'aide de l'algorithme d'Euclide montrer que 17 et 40 sont premiers entre eux.**
   Appliquons l'algorithme d'Euclide :

	$a = 40$
	$b = 17$
$40 = 2 \times 17 + 6$	$r_1 = 6$
$17 = 2 \times 6 + 5$	$r_2 = 5$
$6 = 1 \times 5 + 1$	$r_3 = 1$
$5 = 5 \times 1 + 0$	$r_0 = 0$

   Le PGCD est égal au dernier reste non nul donc $\mathrm{PGCD}(17,40) = 1$: 17 et 40 sont premiers entre eux.

2. **En déduire une solution particulière (x_0, y_0) de (E).**
   En remontant les égalités précédentes, on obtient :
   $6 - 5 = 1$
   $6 - (17 - 2 \times 6) = 1$
   $6 - 17 + 2 \times 6 = 1$
   $3 \times 6 - 17 = 1$
   $3 \times (40 - 2 \times 17) - 17 = 1$
   $3 \times 40 - 6 \times 17 - 17 = 1$
   $3 \times 40 - 7 \times 17 = 1$
   $17(-7) - 40(-3) = 1$
   Cette dernière égalité est de la forme $17x_0 - 40y_0 = 1$ avec $\mathbf{(x_0, y_0) = (-7, -3)}$.

3. Résoudre (E) : $17x - 40y = 1$.

Analyse

Soit (x, y) un couple solution de (E), on a : $17x - 40y = 1$. Or, $17x_0 - 40y_0 = 1$, donc :

$17x - 40y = 17x_0 - 40y_0 \Leftrightarrow 17x - 17x_0 = 40y - 40y_0 \Leftrightarrow 17(x - x_0) = 40(y - y_0)$ $(*)$

On a : $17|(x - x_0)$ et $17(x - x_0) = 40(y - y_0)$, donc : $17|40(y - y_0)$.

On a : $17|40(y - y_0)$ avec 17 et 40 premiers entre eux donc d'après le théorème de GAUSS on en déduit $17|y - y_0$: il existe $k \in \mathbb{Z}$ tel que : $y - y_0 = 17k$, c'est-à-dire tel que : $y = y_0 + 17k$.

Remplaçons dans $(*)$: $17(x - x_0) = 40 \times 17k \Leftrightarrow x - x_0 = 40k \Leftrightarrow x = x_0 + 40k$.

Synthèse

Considérons un couple de la forme $(x_0 + 40k, y_0 + 17k)$, on a :

$$17(x_0 + 40k) - 40(y_0 + 17k) = 17x_0 - 40y_0 + 17 \times 40 \times k - 17 \times 40 \times k$$
$$= 17x_0 - 40y_0 = 1, (x_0, y_0) \text{ étant un couple solution de } (E)$$

Résumons : $17(x_0 + 40k) - 40(y_0 + 17k) = 1$, donc $(x_0 + 40k, y_0 + 17k)$ est un couple solution de (E).

Conclusion

Les solutions de (E) sont les couples $(-7 + 40k, -3 + 17k)$ où $k \in \mathbb{Z}$.

4. Déduire de ce qui précède que 17 admet un unique inverse modulo 40 strictement compris entre 35 et 75, en donner la valeur.

Soit (x, y) un couple solution de (E), on a : $17x - 40y = 1$, donc en raisonnant modulo 40 on en déduit : $17x - 0y \equiv 1\ [40]$, c'est-à-dire : $17x \equiv 1\ [40]$, on en déduit que x est un inverse de 17 modulo $[40]$. D'après **3.**, il existe $k \in \mathbb{Z}$ tel que : $x = -7 + 40k$, or on exige que $20 < x < 35$, donc on cherche la(les) valeur(s) de k tels que :

$$35 < -7 + 40k < 75 \Leftrightarrow 35 + 7 < -7 + 40k + 7 < 75 + 7 \Leftrightarrow 42 < 40k < 82$$

Le seul multiple de 40 strictement compris entre 42 et 82 est 80, atteint pour $k = 2$.

On a alors : $x = -7 + 40(2) = -7 + 80 = 73$.

L'unique inverse modulo 40 de 17 compris entre 35 et 75 est : 73.

BONUS **Pour $a \in \mathbb{Z}$, déterminer $\text{PGCD}(3a + 5, 7a + 6)$.**

Soit $a \in \mathbb{Z}$, on a :

$$\text{PGCD}(3a + 5, 7a + 6) = \text{PGCD}\big(3a + 5, 7a + 6 - 2(3a + 5)\big)$$
$$= \text{PGCD}(3a + 5, 7a + 6 - 6a - 10) = \text{PGCD}(3a + 5, a - 4)$$
$$= \text{PGCD}(3a + 5 - 3(a - 4), a - 4) = \text{PGCD}(3a + 5 - 3a + 12, a - 4)$$
$$= \text{PGCD}(17, a - 4)$$

Or, les seuls diviseurs positifs de 17 sont 1 et 17 donc $\text{PGCD}(17, a - 4) \in \{1; 17\}$.

Deux cas seulement peuvent se présenter :

• si $17|a - 4$, autrement dit si $a \equiv 4\ [17]$, alors on a : $17 > 0$ et $17|a - 4$ donc $\text{PGCD}(17, a - 4) = 17$

• si 17 ne divise pas $a - 4$, autrement dit si $a \not\equiv 4\ [17]$, alors $\text{PGCD}(17, a - 4) \neq 17$, or $\text{PGCD}(17, a - 4) \in \{1; 17\}$, donc $\text{PGCD}(17, a - 4) = 1$.

Résumons :

Si $a \equiv 4\ [17]$, alors : $\text{PGCD}(3a + 5, 7a + 6) = 17$, sinon : $\text{PGCD}(3a + 5, 7a + 6) = 1$.