

1. a. Si d n'est pas multiple de $PGCD(a; b)$, on ne peut pas sortir de la boucle car quels que soient u et v , $a \times u + b \times v \neq d$. Donc l'algorithme ne s'arrête pas.

Cet algorithme cherche à déterminer une solution particulière $(u; v)$ de l'équation $a \times u + b \times v = d$.

- b. L'algorithme précédent donne comme solution $u = 5$ et $v = -2$ ($u = -2$ et $v = 1$ est aussi une solution pertinente, obtenue par l'algorithme avec $a = 7$ et $b = 3$)

$x_0 = 5 \times 10^{2n}$ et $y_0 = -2 \times 10^{2n}$ est donc une solution particulière de (E) .

- c. $3x + 7y = 10^{2n} \Leftrightarrow 3x + 7y = 3 \times 5 \times 10^{2n} + 7 \times (-2) \times 10^{2n} \Leftrightarrow 3(x - 5 \times 10^{2n}) = -7(y + 2 \times 10^{2n})$

Cette dernière équation implique $7 \mid 3(x - 5 \times 10^{2n})$ or 7 et 3 sont premiers entre eux donc d'après le théorème de Gauss $7 \mid (x - 5 \times 10^{2n})$ et il existe un entier k tel que

$x - 5 \times 10^{2n} = 7k \Leftrightarrow x = 5 \times 10^{2n} + 7k$. En remplaçant dans l'équation précédente, on obtient

$3(7k) = -7(y + 2 \times 10^{2n}) \Leftrightarrow y = -2 \times 10^{2n} - 3k$. On vérifie immédiatement que quel que soit

l'entier k , le couple $(5 \times 10^{2n} + 7k; -2 \times 10^{2n} - 3k)$ est solution de (E) . C'est donc l'ensemble cherché.

2. a. $100 = 7 \times 14 + 2$ donc $100 \equiv 2(7)$.

b. D'une part, $10^{2n} = (10^2)^n = 100^n$ et $100 \equiv 2(7)$ donc $10^{2n} \equiv 2^n(7)$. D'autre part, pour tout entier y , $7y^2 \equiv 0(7)$ donc $3x^2 + 7y^2 \equiv 3x^2(7)$. Donc si $3x^2 + 7y^2 = 10^{2n}$ alors $3x^2 \equiv 2^n(7)$.

c. On a :

Reste de la division euclidienne de x par 7	1	2	3	4	5	6
Reste de la division euclidienne de $3x^2$ par 7	3	5	6	6	5	3

d. $2^1 = 2 \equiv 2(7)$, $2^2 = 4 \equiv 4(7)$ et $2^3 = 8 \equiv 1(7)$. Par ailleurs, pour tout entier n , il existe des entiers q et r tels que $n = 3q + r$ avec $r \in \{0; 1; 2\}$. Donc $2^n = 2^{(3q+r)} = (2^3)^q \times 2^r \equiv 2^r(7)$.

Comme $r \in \{0; 1; 2\}$, ceci prouve que 2^n est congru à 1, 2 ou 4 modulo 7.

la question précédente montre que pour tout entier x , $3x^2$ est congru à 3, 5 ou 6 modulo 7 et donc, $3x^2$ et 2^n ne peuvent pas être congrus modulo 7 et l'équation (G) n'a donc pas de solution.