Correction du devoir à la maison n°1

Exercice 1.

1. **a.** $u_1 = 5 \times u_0 + 12 = 57 = 3 \times 19$, $u_2 = 5u_1 + 12 = 297 = 3 \times 99$ et $u_3 = 1497 = 3 \times 499$ donc ces entiers sont tous divisibles par 3.

   b. On considère, pour tout $n \in \mathbb{N}$, la proposition P_n : « u_n est divisible par 3 ».
   Comme $u_0 = 9 = 3 \times 3$, P_0 est vraie.
   Soit $k \in \mathbb{N}$. On suppose que P_k est vraie. Ainsi, 3 divise u_k. Or, $12 = 4 \times 3$ donc 3 divise 12. Dès lors, 3 divise toute combinaison linéaire de u_k et de 12 donc, en particulier, 3 divise $5u_k + 12$ c'est-à-dire 3 divise u_{k+1}. Ainsi, P_{k+1} est vraie.
   On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, 3 divise u_n.

2. Supposons que, pour tout $n \in \mathbb{N}$, d divise u_n. Alors, en particulier, d divise u_0 c'est-à-dire d divise a.
   Réciproquement, supposons que d divise a. Montrons par récurrence que, pour tout $n \in \mathbb{N}$, d divise u_n.
   On considère, pour tout $n \in \mathbb{N}$, la proposition Q_n : « u_n est divisible par d ».
   Comme $u_0 = a$, par hypothèse, Q_0 est vraie.
   Soit $k \in \mathbb{N}$. On suppose que Q_k est vraie. Ainsi, d divise u_k. Or, par hypothèse, d divise 12 donc d divise toute combinaison linéaire de u_k et de 12 et, en particulier, d divise $5u_k + 12$ c'est-à-dire d divise u_{k+1}. Ainsi, Q_{k+1} est vraie.
   On a donc montré par récurrence que, pour tout $n \in \mathbb{N}$, d divise u_n.
   Finalement, on a bien établi l'équivalence entre les deux propositions.

Exercice 2.

1. Déterminer q et Q dans chacun des cas suivants :

   a. $a - 1 = 16 = 3 \times 5 + 1$ donc $q = 3$ et $ab - 1 = 84 = 3 \times 5^2 + 9$ donc $Q = 3$.

   b. $a - 1 = 28 = 2 \times 12 + 4$ donc $q = 2$ et $ab - 1 = 347 = 2 \times 12^2 + 59$ donc $Q = 2$;

   c. $a - 1 = 124 = 7 \times 17 + 5$ donc $q = 7$ et $ab - 1 = 2124 = 7 \times 17^2 + 101$ donc $Q = 7$..

2. On conjecture que $Q = q$.
   Par définition, il existe un entier r tel que $a = bq + r$ et $0 \leqslant r < b$. Dès lors,
   $$ab - 1 = (a - 1)b + b - 1 = (bq + r)b + b - 1 = b^2 q + (r + 1)b - 1.$$
   Or, $0 \leqslant r < b$ donc $1 \leqslant r + 1 < b + 1$ c'est-à-dire $1 \leqslant r + 1 \leqslant b$. Dès lors, $b \leqslant (r + 1)b < b^2$ et donc $0 \leqslant b - 1 \leqslant (r + 1)b - 1 < b^2 - 1$. Ainsi, $ab - 1 = b^2 q + (r + 1)b - 1$ est la division euclidienne de $ab - 1$ par b^2 donc $Q = q$.

3. Soit $n \in \mathbb{N}$. Déterminer, en fonction de q, le quotient dans la division euclidienne de $ab^n - 1$ par b^{n+1}.

4. De même,
   $$ab^n - 1 = (a - 1)b^n + b^n - 1 = (bq + r)b^n + b^n - 1 = b^{n+1} q + (r + 1)b^n - 1.$$
   Or, $0 \leqslant r < b$ donc $1 \leqslant r + 1 < b + 1$ c'est-à-dire $1 \leqslant r + 1 \leqslant b$. Dès lors, $b^n \leqslant (r + 1)b^n < b^{n+1}$ et donc $0 \leqslant b^n - 1 \leqslant (r + 1)b^n - 1 < b^{n+1} - 1$. Ainsi, $ab^n - 1 = b^{n+1} q + (r + 1)b^n - 1$ est la division euclidienne de $ab^n - 1$ par b^{n+1} donc le quotient dans la division euclidienne de $ab^n - 1$ par b^{n+1} est q.

Exercice 3 (facultatif). Supposons que $2^b - 1$ divise $2^a + 1$.

Écrivons la division euclidienne de a par b : il existe un entier $q \geqslant 0$ et un entier r tels que $a = bq + r$ avec $0 \leqslant r < b$. Dès lors,

$$2^a + 1 = 2^{bq+r} + 1 = 2^r(2^{bq} - 1) + 2^r + 1.$$

Or,

$$\sum_{k=0}^{q-1} (2^b)^k = \frac{1 - (2^b)^q}{1 - 2^b} = \frac{2^{bq} - 1}{2^b - 1}$$

Ainsi, $2^{bq} - 1 = (2^b - 1) \sum_{k=0}^{q-1} (2^b)^k$. Or, $\sum_{k=0}^{q-1} (2^b)^k$ est une somme d'entiers donc c'est un entier et ainsi $2^b - 1$ divise $2^{bq} - 1$. Par suite, comme $2^r + 1 = 2^a + 1 - 2^r(2^{bq} - 1)$, $2^b - 1$ divise $2^r + 1$ et donc, comme $2^r + 1 \geqslant 0$, $2^b - 1 \leqslant 2^r + 1$. Or, $r < b$ donc il existe un entier $c > 0$ tel que $b = r + c$ et ainsi $2^{r+c} - 1 \leqslant 2^r + 1$. Dès lors, $2^{r+c} - 2^r \leqslant 2$ donc $2^r(2^c - 1) \leqslant 2$. Comme $c > 0$, $2^c - 1$ est un diviseur positif impair de 2 donc $2^c - 1 = 1$ i.e. $c = 1$. Par suite, $2^r \leqslant 2$ donc $r \leqslant 1$ et ainsi $b = r + c \leqslant 2$, ce qui contredit l'hypothèse $b > 2$.

On aboutit à une absurdité donc $2^b - 1$ ne divise pas $2^a + 1$.