Correction du devoir
Du jeudi 8 avril 2021

EXERCICE 1

Critère d'arrêt **(3 points)**

1) « Si un nombre n n'est pas premier alors, il admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$ ».

   On peut aussi utiliser la contraposée : « si un nombre n n'admet pas de diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$ alors, n est premier. »

2) Pour 317 ($\sqrt{317} \approx 17,18$), on teste les diviseurs premiers : 2, 3, 5, 7, 11, 13 et 17.
   - D'après les règles de divisibilité, 317 n'est pas divisible par 2, 3, 5 et 11.
   - $317 = 7 \times 45 + 2$, $317 = 13 \times 24 + 5$ et $317 = 17 \times 18 + 11$, donc 317 n'est pas divisible par 7, 13 et 17.

   Conclusion : D'après la contraposée du critère d'arrêt 317 est premier.

   Pour 437 ($\sqrt{437} \approx 20,90$), on teste les diviseurs premiers : 2, 3, 5, 7, 11, 13, 17, 19.
   - D'après les règles de divisibilité, 437 n'est pas divisible par 2, 3, 5 et 11.
   - $437 = 7 \times 62 + 3$, $437 = 13 \times 33 + 8$, $437 = 17 \times 25 + 12$, $437 = 19 \times 23$ donc 437 est divisible par 19.

   Conclusion : D'après le critère d'arrêt 437 n'est pas premier.

EXERCICE 2

Décomposition **(3 points)**

On simplifie la fraction à l'aide d'une décomposition en facteurs premiers :

$$\frac{a}{b} = \frac{5\,292}{5\,544} = \frac{2^2 \times 3^3 \times 7^2}{2^3 \times 3^2 \times 7 \times 11} = \frac{3 \times 7}{2 \times 11} = \frac{21}{22}$$

On décompose 903 en facteurs premiers : $903 = 3 \times 7 \times 43$.

On a alors : $a + b = 903 \overset{\div b}{\Leftrightarrow} \frac{a}{b} + 1 = \frac{3 \times 7 \times 43}{b} \Leftrightarrow \frac{21}{22} + 1 = \frac{21 \times 43}{b} \Leftrightarrow$
$\frac{43}{22} = \frac{21 \times 43}{b} \Leftrightarrow b = 21 \times 22 = 462 \Rightarrow a = 903 - 462 = 441.$

EXERCICE 3

Nombre de diviseurs **(3 points)**

On a : $18 = 2 \times 3^2$.

Comme on ne peut décomposer 10 et 21 en plus de deux facteurs, a et b n'ont comme facteurs primaires que 2 et 3.

1) b a 10 diviseurs et $10 = 2 \times 5$.
   La seule configuration possible pour b est : $b = 2^{2-1} \times 3^{5-1} = 2 \times 3^4 = 162$.

2) a a 21 diviseurs et $21 = 3 \times 7$, les deux configurations possibles pour a sont :

- $a = 2^{3-1} \times 3^{7-1} = 2^2 \times 3^6$ qui est à rejeter car alors $\text{pgcd}(a, b) = 2 \times 3^4 = 162$ et
- $a = 2^{7-1} \times 3^{3-1} = 2^6 \times 3^2 = 576$ qui convient car $\text{pgcd}(a, b) = 18$.

Conclusion : les seuls entiers possibles sont 576 et 162.

EXERCICE 4

Autour du théorème de Fermat **(6 points)**

1) a) p est premier et ne divise pas 2 donc d'après le théorème de Fermat : $2^{p-1} \equiv 1\ (p)$.

b) Si k divise n, alors $n = kd$ avec $d \in \mathbb{N}$, on a alors :
$2^n = 2^{kd} \equiv (2^k)^d \overset{2^k \equiv 1}{\equiv} 1^d \equiv 1\ (p)$.

c) On divise n par b : $n = bq + r$ avec $0 \leqslant r < b$. On a alors :
$2^n \equiv 2^{bq+r} \equiv (2^b)^q \times 2^r \equiv 1^q \times 2^r \equiv 2^r \equiv 1\ (p)$.
Comme $r < b$, on a $r = 0$ car sinon b ne serait pas le plus petit entier vérifiant la propriété. On en déduit alors que b divise n.

2) a) A est multiple de p donc $2^q - 1 \equiv 0\ (p) \iff 2^q \equiv 1\ (p)$.

b) Si $p = 2$ alors 2^q est pair donc $2^q \equiv 0\ (p)$. Contradiction.
On en déduit que p est impair.

c) D'après le 1c), b divise q et comme q est premier alors $b = 1$ ou $b = q$.
$b \neq 1$ car $2^1 \equiv 2 \not\equiv 1\ (p)$ avec p impair, donc $b = q$.

d) D'après le 1a), $2^{p-1} \equiv 1\ (p)$ donc $q = b$ divise $(p - 1)$.
Comme p est impair, $(p - 1)$ est pair. Les entiers 2 et q divise $(p - 1)$, comme $\text{pgcd}(2, q) = 1$, d'après le corollaire du théorème de Gauss, $2q$ divise $(p - 1)$ et donc $p \equiv 1\ (2q)$.

3) Soit p un facteur premier de A_1, d'après le 2d), p est de la forme $(2q)m + 1 = 34m + 1$.
$A_1 = 131\,071$ et $\sqrt{A_1} \approx 362$.

103, 137, 239 et 307 ne divise pas A_1, d'après le critère d'arrêt et 2d), A_1 est premier.

EXERCICE 5

Equation **(5 point)**

1) a) On a le tableau de congruence suivant :

$n \equiv \ldots\ (9)$	0	1	2	3	4	5	6	7	8
$n^2 \equiv \ldots\ (9)$	0	1	4	0	7	7	0	4	1

b) Comme $a^2 - 250\,507 = b^2$ est un carré, les restes possibles sont, d'après le tableau de congruence : 0, 1, 4, 7.

c) $250\,507 \equiv 2 + 5 + 5 + 7 \equiv 19 \equiv 1\ (9)$.
L'équation (E) modulo 9 devient : $a^2 - 1 \equiv b^2\ (9)$. Par disjonction des cas :
- $b^2 \equiv 0\ (9) \implies a^2 \equiv 1\ (9)$
- $b^2 \equiv 1\ (9) \implies a^2 \equiv 2\ (9)$ impossible
- $b^2 \equiv 4\ (9) \implies a^2 \equiv 5\ (9)$ impossible

- $b^2 \equiv 7\ (9) \ \Rightarrow\ a^2 \equiv 8\ (9)$ impossible

La seule solution qui convient est $a^2 \equiv 1\ (9) \ \Rightarrow\ a \equiv 1\ (9)$ ou $a \equiv -1 \equiv 8\ (9)$.

2) D'après (E), $a^2 \geqslant 250\,507 \ \Rightarrow\ a \geqslant \sqrt{250\,507} \geqslant 501$.
501 n'est pas solution car $501^2 - 250\,507 = 494$ qui n'est pas un carré donc $a > 501$.

3) a) $503 \equiv 8\ (9)$ et $505 \equiv 1\ (9)$ comme a est congru à 1 ou 8 modulo 9 alors par transitivité, a est congru à 503 ou 505 modulo 9.

b)
- Pour $k = 0$: $a = 505$ donc $a^2 - 250\,507 = 4518$ qui n'est pas un carré.
- Pour $k = 1$: $a = 514$ donc $a^2 - 250\,507 = 117^2$.

Donc $(514\ ;\ 117)$ est solution de (E).

4) a) D'après 3) : $250\,507 = 514^2 - 117^2 = (514 - 117)(514 + 117) = 397 \times 631$.

b) À l'aide du critère d'arrêt, on montre facilement que 397 et 631 sont premiers. Cette écriture est la décomposition en facteurs premiers de 250 507, elle est donc unique.