

Exercice 1 : On considère les entiers naturels  $M_n = 2^n - 1$  avec  $n \in \mathbb{N}$ .

1. Trois nombres premiers de la forme  $2^n - 1$  : si  $n = 2$ ,  $M_2 = 3$  est premier,  $M_3 = 7$  est premier,  $M_5 = 31$  est premier.

2. a) Pour tout entier naturel  $n$  et tout réel  $x$ ,

$$(x-1)(x^{n-1} + x^{n-2} + \dots + x + 1) = x^n + x^{n-1} + x^{n-2} + \dots + x - x^{n-1} - x^{n-2} - \dots - x - 1 = x^n - 1.$$

b) Si  $n$  n'est pas premier, alors il existe deux entiers naturels  $p$  et  $q$  distincts de 1 tels que  $n = pq$ .

Alors,  $M_n = 2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \dots + 2^p + 1)$  qui est divisible par  $2^p - 1 \neq 1$  puisque  $p \neq 1$ . Donc  $M_n$  n'est pas premier.

3. a) Si  $p$  est un diviseur premier de  $M_n$ , alors il existe un entier naturel  $q$  tel que  $M_n = pq$ .

Donc  $2^n = pq + 1$ , et  $2^n \equiv 1 (p)$ .

b) On sait que  $2^s \equiv 1 (p)$ , et  $n = sq + r$  la division euclidienne de  $n$  par  $s$ , donc  $0 \leq r < s$ .

$$M_n = 2^n - 1 = 2^{sq+r} - 1 = (2^s)^q \times 2^r - 1 \equiv 2^r - 1 \equiv 0 (p). \text{ Donc } 2^r \equiv 1 (p).$$

c) Comme  $0 \leq r < s$  et  $s$  est le plus petit entier tel que  $2^s \equiv 1 (p)$ , alors  $r = 0$  et  $s$  divise  $n$ .

Exercice 2 : Partie A : 1. Démonstration par l'absurde: supposons que  $a$  et  $b$  aient la même parité.

Alors  $a^2$  et  $b^2$  ont la même parité, et donc  $N$  est pair; car la différence de deux entiers de même parité est paire.

Comme  $N$  est impair, ceci est impossible. Donc  $a$  et  $b$  n'ont pas la même parité.

2. Il suffit d'écrire  $N = (a-b)(a+b) = pq$ .

3. Si  $a$  et  $b$  n'ont pas la même parité, alors  $p = a-b$  et  $q = a+b$  sont impairs.

En effet :  $a = 2k$  et  $b = 2k' + 1$ , avec  $k$  et  $k'$  dans  $\mathbb{N}$ , alors  $p = a-b = 2(k-k') + 1$  et  $q = a+b = 2(k+k') + 1$ .

Partie B : On considère l'équation (E) :  $a^2 - 250507 = b^2$  où  $a$  et  $b$  sont des entiers naturels.

1. Dans un tableau, les restes possibles de  $x$  modulo 9, puis ceux de  $x^2$  modulo 9.

$x$	0	1	2	3	4	5	6	7	8
$x^2$	0	1	4	0	7	7	0	4	1

2. Sachant que  $b^2 = a^2 - 250507$ , les restes possibles modulo 9 de  $a^2 - 250507$  sont 0, 1, 4 et 7; sachant que  $250507 \equiv 1 (9)$ ,

alors  $a^2 - 250507 \equiv a^2 - 1 \equiv b^2 (9)$ , soit  $a^2 \equiv b^2 + 1 (9)$ , et les restes possibles modulo 9 de  $a^2$  sont 1, 2, 5 et 8.

3. Parmi les restes possibles modulo 9 de  $a^2$ , le seul reste d'un carré est 1. Et d'après le tableau, les restes possibles de  $a$  modulo 9 sont 1 et 8.

4. a)  $a = 514 = 9 \times 57 + 1 \equiv 1 (9)$  est une solution possible.

b) Dans ce cas,  $b^2 = a^2 - 250507 = 514^2 - 250507 = 13689$  et  $b = \sqrt{13689} = 117$ .

5. On peut écrire  $250507 = (a-b)(a+b) = 397 \times 631$ .

Question hors barème : Les deux facteurs sont des nombres premiers. Cette décomposition est unique puisque c'est la décomposition en facteurs premiers de 250507.

Exercice 3 : 1. a) Pour tout entier naturel  $m$ ,  $m$  s'écrit  $3k$ ,  $3k+1$  ou  $3k+2$ . Si  $p$  est premier supérieur à 7, alors  $p$  n'est pas un multiple de 3, et  $p$  s'écrit  $3k+1$  ou  $3k+2 \equiv -1 (3)$ . Donc  $p$  est congru à  $-1$  ou à  $1$  modulo 3.

b) Ainsi,  $p^4 \equiv (-1)^4 \equiv 1 (3)$  ou  $p^4 \equiv 1^4 \equiv 1 (3)$ . Donc  $n = p^4 - 1 \equiv 0 (3)$ . Et  $n$  est divisible par 3.

2. a) Comme  $p$  est impair, il existe un entier naturel  $k$  tel que  $p = 2k+1$ .

$$\text{D'où } p^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1).$$

b) On sait que pour tout entier naturel  $k$ , un des entiers consécutifs  $k$  ou  $k+1$  est pair, donc  $k(k+1)$  est pair égal à  $2d$ , d'où  $p^2 - 1 = 4k(k+1) = 8d$  est divisible par 8. De plus, comme  $p$  est impair,  $p^2$  aussi et  $p^2 + 1$  est pair  $= 2d'$ .

$$\text{Donc } n = p^4 - 1 = (p^2 - 1)(p^2 + 1) = 16dd' \text{ et } n \text{ est divisible par } 16.$$

3. Les restes possibles de la division euclidienne de  $p$  par 5 sont 1, 2, 3 ou 4. Puisque  $p$  n'est pas un multiple de 5.

Si  $p \equiv 1 (5)$ , alors  $p^4 \equiv 1 (5)$  et  $n \equiv 0 (5)$ .

Si  $p \equiv 2 (5)$ , alors  $p^4 \equiv 16 \equiv 1 (5)$  et  $n \equiv 0 (5)$ .

Si  $p \equiv 3 (5)$ , alors  $p^4 \equiv 81 \equiv 1 (5)$  et  $n \equiv 0 (5)$ .

Si  $p \equiv 4 (5)$ , alors  $p^4 \equiv 256 \equiv 1 (5)$  et  $n \equiv 0 (5)$ .

Ainsi 5 divise  $n$ .

4. On sait que  $n$  est divisible par 3, 16 et 5 qui sont premiers entre eux, donc  $n$  est divisible par  $3 \times 16 \times 5 = 240$ .