

On rappelle la propriété, connue sous le nom de petit théorème de Fermat :

« Soit  $p$  un nombre premier et  $a$  un entier naturel premier avec  $p$  ; alors  $a^{p-1} - 1$  est divisible par  $p$  ».

**1.** Soit  $p$  un nombre premier impair.

**a.** Montrer qu'il existe un entier naturel  $k$ , non nul, tel que  $2^k \equiv 1(p)$ .

**b.** Soit  $k$  un entier naturel non nul tel que  $2^k \equiv 1(p)$  et soit  $n$  un entier naturel. Montrer que, si  $k$  divise  $n$ , alors  $2^n \equiv 1(p)$ .

**c.** Soit  $b$  tel que  $2^b \equiv 1(p)$ ,  $b$  étant le plus petit entier non nul vérifiant cette propriété. Montrer, en utilisant la division euclidienne de  $n$  par  $b$ , que si  $2^n \equiv 1(p)$ , alors  $b$  divise  $n$ .

**2.** Soit  $q$  un nombre premier impair et le nombre  $A = 2^q - 1$ . On prend pour  $p$  un facteur premier de  $A$ .

**a.** Justifier que :  $2^q \equiv 1(p)$ .

**b.** Montrer que  $p$  est impair.

**c.** Soit  $b$  tel que  $2^b \equiv 1(p)$ ,  $b$  étant le plus petit entier non nul vérifiant cette propriété. Montrer, en utilisant 1. que  $b$  divise  $q$ . En déduire que  $b = q$ .

**d.** Montrer que  $q$  divise  $p - 1$ , puis montrer que  $p \equiv 1(2q)$ .

**3.** Soit  $A_1 = 2^{17} - 1$ . Voici la liste des nombres premiers inférieurs à 400 et qui sont de la forme  $34m+1$ , avec  $m$  entier non nul : 103, 137, 239, 307. En déduire que  $A_1$  est premier.

## Corrigé

**1.** Soit  $p$  un nombre premier impair.

**a.**  $p$  étant un entier impair, il n'est pas divisible par 2. Comme 2 est premier, si 2 ne divise pas  $p$ , alors 2 est premier avec  $p$ .

Le petit théorème de Fermat (avec  $a = 2$ ) donne alors  $2^{p-1} - 1 \equiv 0 \pmod{p} \Leftrightarrow 2^{p-1} \equiv 1 \pmod{p}$ , avec  $p-1 > 2$ .

Ainsi, **l'entier  $k = p-1$  est un entier naturel, non nul, tel que  $2^k \equiv 1 \pmod{p}$ .**

**b.** Soit  $k$  un entier naturel non nul tel que  $2^k \equiv 1 \pmod{p}$ .

Soit  $n$  un entier naturel tel que  $k$  divise  $n$ . Alors, il existe un entier  $c$  tel que  $n = kc$ .

Dans ce cas,  $2^n = 2^{kc} = (2^k)^c$  et comme  $2^k \equiv 1 \pmod{p}$ , on obtient  $2^n = (2^k)^c \equiv 1^c \pmod{p} \equiv 1 \pmod{p}$ .

**c.** Soit  $b$  tel que  $2^b \equiv 1 \pmod{p}$ ,  $b$  étant le plus petit entier non nul vérifiant cette propriété.

Effectuons la division euclidienne de  $n$  par  $b$  : il existe donc des entiers naturels  $q$  et  $r$  tels que 
$$\begin{cases} n = bq + r \\ 0 \leq r < b \end{cases}.$$

Supposons donc que  $2^n \equiv 1 \pmod{p}$  (et montrons que  $b$  divise  $n$ ) : il vient  $2^{bq+r} \equiv 1 \pmod{p} \Leftrightarrow (2^b)^q 2^r \equiv 1 \pmod{p} \Leftrightarrow 2^r \equiv 1 \pmod{p}$  puisque  $2^b \equiv 1 \pmod{p}$ .

On a donc  $2^r \equiv 1 \pmod{p}$  avec  $0 \leq r < b$ ,  $b$  étant par hypothèse le plus petit entier non nul vérifiant cette propriété.

Donc  $r = 0$  et  $n = bq$ , cad que  $b$  divise  $n$ .

**2.** Soit  $q$  un nombre premier impair et le nombre  $A = 2^q - 1$ . On prend pour  $p$  un facteur premier de  $A$ .

**a.**  $p$  étant un facteur premier de  $A$  il divise  $A$  et on a  $A = 2^q - 1 \equiv 0 \pmod{p}$  et donc  $2^q \equiv 1 \pmod{p}$ .

**b.**  $A = 2^q - 1$  donc  $A \equiv 1 \pmod{2}$  ainsi  $A$  est impair. Comme  $p$  est un facteur (premier) de  $A$ , il est impair (sinon  $A$  serait divisible par 2).

**c.** Soit  $b$  tel que  $2^b \equiv 1 \pmod{p}$ ,  $b$  étant le plus petit entier non nul vérifiant cette propriété.

- Prouvons que  $b$  divise  $q$  : par définition de  $b$ , la question 1 nous permet d'affirmer que comme  $2^q \equiv 1 \pmod{p}$  (2.a),  **$b$  divise  $q$** .
- Mais par hypothèse,  $q$  est un nombre premier donc si  $b$  divise  $q$ , on a  $b = 1$  ou  $b = q$ .  
Or  $2^b \equiv 1 \pmod{p}$  donc si  $b = 1$  on obtient  $2^1 \equiv 1 \pmod{p} \Leftrightarrow 1 \equiv 0 \pmod{p} \Leftrightarrow p \mid 1$  ce qui est absurde puisque  $p$  est plus grand que 1.  
Donc  $b = q$ .

**d.** Montrons que  $q$  divise  $p-1$ , puis que  $p \equiv 1 \pmod{2q}$ .

- D'après la question précédente  $b = q$  est le plus petit entier naturel non nul tel que  $2^b \equiv 1 \pmod{p}$ .  
Comme d'après le 1.a,  $2^{p-1} \equiv 1 \pmod{p}$ , on a d'après le 1.c,  $b = q$  divise  $p-1$ .
- Nous savons que  $p$  est impair donc  $p-1$  est pair. Ainsi **2 divise  $p-1$** . Mais on a aussi  **$q$  divise  $p-1$** .  
Comme  $q$  est un premier impair,  **$q$  est premier avec 2**. D'après un corollaire du théorème de Gauss, on sait alors que  $2q$  divise  $p-1$ . Ainsi,  $p-1 \equiv 0 \pmod{2q} \Leftrightarrow p \equiv 1 \pmod{2q}$ .

**3.** Soit  $A_1 = 2^{17} - 1$ .

Remarquons déjà que  $q = 17$  est un nombre premier impair.

D'après la partie 2, nous savons que **si  $p$  est un facteur premier de  $A_1 = 2^{17} - 1$  alors  $p \equiv 1 \pmod{2 \times 17}$** .

La contraposée de cette propriété « **si  $p \not\equiv 1 \pmod{34}$  alors  $p$  n'est pas un facteur premier de  $A_1 = 2^{17} - 1$**  », nous permet de rechercher les facteurs premiers de  $A$  parmi les nombres 103, 137, 239 et 307.

A l'aide de la calculatrice, on vérifie rapidement que ces nombres ne divisent pas  $A$  :  $A$  n'admet donc aucun facteur premier (autre que lui-même), il est donc premier.