

1. Soit $P(a) = a^n - 1$, où a est un entier différent de 1, et n un entier supérieur ou égal à 1.
 - a. Calculer $1 + a + a^2 + \dots + a^{n-1}$
 - b. Montrer que $P(a)$ peut s'écrire sous la forme $k(a-1)$, où k est un entier.
 2. a. Montrer que : $a^{2 \times 280} - 1 = k(a^2 - 1)$, avec k entier, puis que $a^{561} - a = k a(a^2 - 1)$
 - b. En utilisant les congruences modulo 3, montrer que $a^{561} - a$ est divisible par 3
 3. a. Montrer que $a^{561} - a = k' a(a^{10} - 1)$ avec k' entier
 - b. En utilisant les congruences modulo 11, montrer que $a^{561} - a$ est divisible par 11.
 4. a. Montrer que $a^{561} - a = k'' a(a^{16} - 1)$ avec k'' entier.
 - b. En utilisant les congruences modulo 17, montrer que $a^{561} - a$ est divisible par 17.
 5. En déduire que a^{561} congru a modulo 561.
- Un entier n non nul différent de 1 et qui n'est pas premier est appelé nombre de Carmichael si, pour tout a entier, n divise $a^n - a$
6. Pourquoi 561 est-il un nombre de Carmichael ?

CORRECTION

1. a. a est un entier différent de 1, donc $1 + a + a^2 + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}$.

b. $1 + a + a^2 + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}$ donc $P(a) = (a - 1) \left(1 + a + a^2 + \dots + a^{n-1} \right)$.

$P(a)$ peut s'écrire sous la forme $k(a-1)$, où $k = 1 + a + a^2 + \dots + a^{n-1}$, a est un entier donc k est un entier.

2. a. $(q-1)(1+q+q^2+\dots+q^{n-1}) = q^n - 1$ donc en appliquant ceci à $q = a^2$ et $n = 280$
 $a^{2 \times 280} - 1 = (a^2)^{280} - 1 = k(a^2 - 1)$, où $k = 1 + (a^2) + (a^2)^2 + \dots + (a^2)^{280-1}$

a est un entier donc k est un entier,

$a^{2 \times 280} - 1 = a^{560} - 1 = k(a^2 - 1)$, donc en multipliant par a : $a(a^{560} - 1) = a k(a^2 - 1)$, soit $a^{561} - a = k a(a^2 - 1)$

b. si a n'est pas divisible par 3, 3 est un nombre premier donc $a^2 \equiv 1$ modulo 3 d'après le petit théorème de Fermat.
 $a^{561} - a = k a(a^2 - 1)$ donc $a^{561} - a \equiv 0$ modulo 3,

si a est divisible par 3, alors $a \equiv 0$ modulo 3 donc $a^{561} \equiv 0$ modulo 3 donc $a^{561} - a \equiv 0$ modulo 3

Dans tous les cas, $a^{561} - a \equiv 0$ modulo 3 donc $a^{561} - a$ est divisible par 3.

3. a. $a^{561} - a = a(a^{560} - 1) = a((a^{10})^{56} - 1)$

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

En appliquant ceci à $q = a^{10}$ et $n = 56$ alors : $(a^{10})^{56} - 1 = (a^{10} - 1)(1 + (a^{10}) + (a^{10})^2 + \dots + (a^{10})^{56-1})$

donc $a^{560} - 1 = k'(a^{10} - 1)$, avec $k' = 1 + (a^{10}) + (a^{10})^2 + \dots + (a^{10})^{55}$

a est un entier donc k' est un entier donc $a^{561} - a = k' a(a^{10} - 1)$ avec k' entier

b. si a n'est pas divisible par 11, 11 est un nombre premier donc $a^{10} \equiv 1$ modulo 11 d'après le petit théorème de Fermat
 $a^{561} - a = k' a(a^{10} - 1)$ avec k' entier donc : $a^{561} - a \equiv 0$ modulo 11

si a est divisible par 11, alors $a \equiv 0$ modulo 11 donc $a^{561} \equiv 0$ modulo 11 donc $a^{561} - a \equiv 0$ modulo 11

Dans tous les cas, $a^{561} - a \equiv 0$ modulo 11 donc $a^{561} - a$ est divisible par 11

4. a. $560 = 16 \times 35$

$a^{561} - a = a(a^{560} - 1) = a((a^{16})^{35} - 1)$

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

En appliquant ceci à $q = a^{16}$ et $n = 35$ alors

$(a^{16})^{35} - 1 = (a^{16} - 1)(1 + (a^{16}) + (a^{16})^2 + \dots + (a^{16})^{35-1})$

donc $a^{560} - 1 = k''(a^{16} - 1)$, avec $k'' = 1 + (a^{16}) + (a^{16})^2 + \dots + (a^{16})^{34}$

a est un entier donc k'' est un entier donc $a^{561} - a = k'' a(a^{16} - 1)$ avec k'' entier

b. si a n'est pas divisible par 17, 17 est un nombre premier donc $a^{16} \equiv 1$ modulo 17 d'après le petit théorème de Fermat
 $a^{561} - a = k'' a(a^{16} - 1)$ donc $a^{561} - a \equiv 0$ modulo 17,

si a est divisible par 17, alors $a \equiv 0$ modulo 17 donc $a^{561} \equiv 0$ modulo 17 donc $a^{561} - a \equiv 0$ modulo 17

Dans tous les cas, $a^{561} - a \equiv 0$ modulo 17 donc $a^{561} - a$ est divisible par 17

5. $561 = 3 \times 11 \times 17$

3 divise $a^{561} - a$ et 11 divise $a^{561} - a$, 3 et 11 sont premiers entre eux donc d'après le théorème de Gauss, 3×11 divise $a^{561} - a$.

33 divise $a^{561} - a$ et 17 divise $a^{561} - a$, 33 et 17 sont premiers entre eux donc, 33×17 divise $a^{561} - a$ d'après le théorème de Gauss donc 561 divise $a^{561} - a$ donc a^{561} congru a modulo 561.

6. Pour tout a entier différent de 1, 561 divise $a^{561} - a$,

si $a = 1$, $a^{561} - a = 0$ donc 561 divise $a^{561} - a$, donc pour tout entier a , 561 divise $a^{561} - a$,

561 est un entier non nul différent de 1 et qui n'est pas premier, pour tout a entier, 561 divise $a^{561} - a$, donc 561 est un nombre de Carmichael.