Theorème d'Euler. FOCUS + SYNTAXE. EULER 01

REPOSE SUR LA PROPRIETE ARITHMETIQUE D'EUCLIDE.

PRINCIPE, RAPPELS:

Si $n \in \mathbb{Z} \neq 0$.

- pour tout entier naturel : a premier avec n

$$a^{\phi(n)} \equiv 1 \mod (n)$$

$$a^{\phi(n)} \equiv \ \%$$

RAPPEL: $a \equiv b \ (\mod n)$

SIGNIFIE

a et b ont le même reste quand ils sont divisé par n → si je fais $\frac{a-b}{n} =$

ex: $a = 7$; $b = 10$; $(c = 22)$

$a \equiv b \ (\mod 3)$ même reste

a est congru de b modulo 3

Car $7 \% 3 = 1$

$10 \% 3 = 1$

$\frac{7-10}{3} = -1$

SYNTAXE CONVENTION (INFORMATIQUE)

$a \% k == b$

$a \equiv b \ (\mod k)$

ex: $10 \% 3 == 1$.

$10 \equiv 1 \ (\mod 3)$

$10 \% 3 = 1$; $1 \% 3 = 1$

modulo = paquet

Euclidienne : $1 \% x$ avec $x \in \mathbb{Z}$ aura toujours un reste de 1

EULER :

$$\boxed{a^{\phi(n)} \equiv 1 \bmod (n)}$$

$\phi(n)$ nombre d'entiers naturels ^{N} inférieurs à n qui sont premiers avec n

⇓

Si n est un entier naturel non nul alors pour tout entier naturel a premier avec n

$n = 10$
$a = 7$

0. J'Ai a et n cause d'arrêt de départ

ex
si $n=10$, $a=7$, trouvons $\phi(n)$ soit $\phi(10)$

1. Quel est le nombre d'entiers naturels compris entre 1 et 10 qui sont premiers avec 10 ?

ETRE PREMIER AVEC x, C'EST QUE LE NOMBRE quand je fais $\frac{x}{\text{NOMBRE}}$ donne un résultat entier n'a qu'un seul diviseur commun avec x, soit PGCD(x, NOMBRE) = 1

ex: NON $10/10 = 1$ | $10/1 = 1$
$10/9 = 1$ | $9/1 = 1$
NON $10/2 = 5$ | $8/1 = 1$ $8/2 = 4$ ↳ 8 et 10 ont 2 comme diviseur commun, il ne sont pas premiers entre eux.
etc...

ON FAIT LE PGCD SUR 1 jusque 10 et on relève que les résultats en 1.

Voici L'ENSEMBLE

2. COMPTER LES ÉLÉMENTS.

$U := \{1;3;7;9\}$ 4 éléments

donc $\phi(10) = 4$

3. REPRODUIRE LA FORMULE D'EULER.

$$\boxed{a^4 \equiv 1 \bmod (10)}, \text{ soit } \boxed{7^4 \equiv 1 \bmod (10)}$$

$7^4 \% 10$ à un reste de 1
$1 \% 10$ à un reste de 1

EULER 02

$7^4 = 2401 = 10 \times 240 + 1$

↳ en effet donc $7^4 \% 10 \rightarrow$ reste 1.

$1 \% 10 \rightarrow$ reste 1. (même reste).

↳ On va démontrer la même chose que ceci mais d'une autre façon qui permettra de généraliser.

$7U = \{7 ; 21 ; 49 ; 63\}$

$1 \times 7 \quad 3 \times 7 \quad 7 \times 7 \quad 9 \times 7$

4. ON MULTIPLIE TOUS LES NOMBRES DE L'ENSEMBLE U par 7.

⚠ Règle sur le produit des congruences

5. EXAMINONS CHAQUE NOMBRE DE CET ENSEMBLE MODULO 10.

Si

$7 \equiv 7 \mod(10)$ ← dans 7, combien de fois 10 ? 0, reste 7 je place 7 à droite de ≡

$21 \equiv 1 \mod(10)$

$49 \equiv 9 \mod(10)$

$63 \equiv 3 \mod(10)$ ← dans 63, 6×10+3, je place 3 à droite.

Réécrire

$63 \% 10 = 3$ $\quad 3 \% 10 = 3$

6. ON MULTIPLIE TOUTES LES CONGRUENCE ... A

$7 \times 21 \times 49 \times 63 \equiv 7 \times 1 \times 9 \times 3 \mod(10)$

7. ON RÉÉCRIT CELA, EN REMETTANT EN MULTIPLE DE 7 A CHAQUE ET EN RANGEANT DANS L'ORDRE CROISSANT DE CHAQUE CÔTÉ DE LA CONGRUENCE.

$(7 \cdot 1) \times (7 \cdot 3) \times (7 \cdot 7) \times (7 \cdot 9) \equiv 1 \times 3 \times 7 \times 9 \mod(10)$

↳ J'AI UN 7^4 du théorème d'Euler ! FACTORISATION.

$7^4 \times (1 \times 3 \times 7 \times 9) \equiv 1 \times 3 \times 7 \times 9 \mod(10)$

8. JE SIMPLIFIE $1 \times 3 \times 7 \times 9$.

$1 \times 3 \times 7 \times 9 = 189 \Rightarrow$ je fais la congruence de 189 $\Rightarrow 189 \equiv 9 \mod(10)$

9. REPREUVRE LA CONJECTURE OBTENUE

$189 \equiv 9 \mod (10)$

↓ 10. Multiplier ce nombre par un nombre qui permet d'obtenir un résultat sur lequel résultat % 10 = 1.

ex: j'ai repéré que $9 \times 9 = 81$

$81 \% 10 = 1$

$189 \times 9 \equiv 9 \times 9 = 81 \equiv 1 \mod (10)$

11. Donc pour simplifier le produit $1 \times 3 \times 7 \times 9$, il suffit de multiplier par 9 des deux côtés, et il restera.

RAPPEL $7^4 \times 189 \equiv 189$

$7^4 \times 189 \times 9 \equiv 189 \times 9 \mod (10)$

donc

$7^4 \equiv 1 \mod (10)$

QUE FAUT-IL CONPREUVRE ?

l'ensemble U, c-a-d $U := \{1,3,7,9\}$

l'ensemble 7U, c-a-d $7U := \{7,21,49,63\}$

- sont identiques à a les regarde modulo 10.
- le produit des nombres qui sont premier à avec 10 peut se simplifier.

CAS GENERAL.

PROP 1 : Si a est un entier naturel premier avec n, alors il existe un entier naturel b tel que $ab \equiv 1 \mod (n)$

REFORMULATION DU THEOREME DE BEZOUT

PROP 2 : Si a_1 et a_2 sont 2 entiers naturels premiers avec n alors le produit $a_1 a_2$ est aussi premier avec n

COROLLAIRE DU TH DE BEZOUT