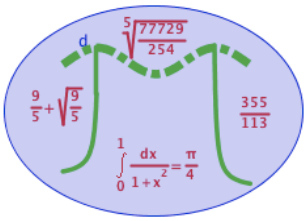

# Le petit théorème de Fermat

Soit p un nombre premier et un entier naturel a non multiple de p.

On a alors : $a^{p-1} \equiv 1$ (p)

## Une démonstration intéressante

Considérons les p-1 premiers multiples de a : .....

Démontrons que si on appelle $r_1, r_2, \ldots, r_{p-1}$ les restes dans la division par p de ces entiers, ces restes sont deux à deux distincts.

Raisonnons pour cela par ..... :

En effet, supposons que ..... pour $i \neq j$ .

On a alors $ai - aj \equiv$ ..... (p) c'est à dire $a(i-j) \equiv$ ..... ; (p) donc $a(i-j)$ serait ..... de p ce qui est impossible car .....

$r_1, r_2, \ldots, r_{p-1}$ sont donc des restes non nuls et deux à deux distincts on a alors

$r_1 \times r_2 \times \ldots \times r_{p-1}$ = ..... = .....

Or on sait que $a \times 2a \times \ldots \times (p-1)a \equiv$ ..... (p)

donc $a \times 2a \times \ldots \times (p-1)a \equiv$ ..... (p)

..... $\equiv$ ..... (p)

..... $\equiv 0$ (p)

..... est donc multiple de p or p et ..... sont premiers entre eux donc d'après le th de Gauss p divise ..... d'où $a^{p-1} \equiv 1$ (p)