

**$p$  et  $q$  sont deux entiers premiers entre eux.**

$x$  est un entier.

On sait :  $x \equiv r \pmod{p}$  et  $x \equiv r \pmod{q}$

Autrement dit : le reste de  $x$  dans la division euclidienne par  $p$  et par  $q$  est le même.

Ou encore :

$x - r$  est un multiple de  $p$ , et, est un multiple de  $q$ .

Conclusion :  $x \equiv r \pmod{pq}$

**Illustration :**

**Un exemple :**

$p = 15$                       et                       $q = 22$

15 et 22 sont premiers entre eux                       $15 = 3 \times 5$  et  $22 = 2 \times 11$  (aucun facteur premier commun aux deux décompositions).

$$\text{PGCD}(15 ; 22) = 1$$

$x = 12\,893$

$$12\,883 = 15 \times 858 + 13 \qquad 12\,883 \equiv 13 \pmod{15}$$

$$12\,883 = 22 \times 585 + 13 \qquad 12\,883 \equiv 13 \pmod{22}$$

Ou encore :  $12\,883 - 13 = 12\,870 = 15 \times 858 = 22 \times 585$

Comme 15 et 22 sont premiers entre eux, on est certain (d'après Gauss) que 15 divise 585 et que 22 divise 858, et que les quotients de 585 par 15 et de 858 par 22 sont égaux.

$$585 = 15 \times 39 \text{ et } 858 = 22 \times 39$$

On obtient :  $12\,883 - 13 = 12\,870 = 15 \times 22 \times 39$

Conclusion :  $12\,883 \equiv 13 \pmod{15 \times 22}$

**Un contre-exemple :**

$p = 6$  et  $q = 14$                        $\text{PGCD}(6 ; 14) = 2$

$$213 = 6 \times 35 + 3 \qquad 213 \equiv 3 \pmod{6}$$

$$213 = 14 \times 15 + 3 \qquad 213 \equiv 3 \pmod{14}$$

$$213 - 3 = 210 = 6 \times 35 = 14 \times 15$$

Or,  $6 \times 14 = 84$

On ne peut pas décomposer 35 (ou 15) de façon à faire apparaître 84

$$6 \times 5 \times 7 = 14 \times 3 \times 5$$

$$213 = 84 \times 2 + 45 \qquad 213 \equiv 45 \pmod{6 \times 14}$$

**Démonstration :**

D'après les données :  $x - r \equiv 0 \pmod{p}$  et  $x - r \equiv 0 \pmod{q}$ .

il existe donc deux entiers  $k$  et  $k'$  tels que  $x - r = pk = qk'$  (1)

$pk = qk'$  et  $p$  et  $q$  premiers entre eux implique qu'il existe un entier  $k''$  tel que  $k' = pk''$  et  $k = qk''$  (Gauss)

En remplaçant dans (1) :  $x - r = pqk''$                       Conclusion :  $x \equiv r \pmod{pq}$