

Rappel de cours

Exercice 1

Trouver 17^{-1} dans $\mathbb{Z}/20\mathbb{Z}$.

On a $\text{pgcd}(17, 20) = 1$ donc l'inverse existe. Il faut trouver x tel que $17.x = 1 \pmod{20}$ (ou $17.x = 1 + k.20$).

Ou bien $17.x + (-k).20 = 1 = \text{pgcd}(17, 20)$. Rebonjour Mr Bezout. Il faut trouver x et k . Donc, n steps.

Trouver le reste de $20/17$.

$$20 = 17.(1) + 3$$

Trouver le reste de $17/3$

$$17 = 3.(5) + 2$$

Trouver le reste de $3/2$

$$3 = 2.(1) + 1$$

Le reste est 1 on arrête. Ensuite on inverse

$$20 + 17.(-1) = 3$$

$$17 + 3.(-5) = 2$$

$$3 + 2.(-1) = 1$$

Et on remonte et on remplace

$$3 + 2.(-1) = 1$$

$$3 + (17 + 3.(-5)).(-1) = 3.(6) + 17(-1) = 1$$

$$(20 + 17.(-1)).(6) + 17(-1) = 20.(6) + 17(-7) = 1$$

On a trouvé $k = 6$ et $x = -7$. Mais l'inverse doit être positif. on calcule $-7 \pmod{20} = 13$ donc $17^{-1} = 13 \pmod{20}$. En effet, $17.13 = 221 = 1 \pmod{20}$.

QED