Exercices Série 5

1) Trouve l'inverse de $14\ mod\ 31$
2) Appliquez l'algorithme d'Euclide étendu pour obtenir le PGCD de 1540 et 546.
3) Appliquez l'algorithme d'exponentiation rapide pour calculer $12^{27}\ mod\ 15$.
4) Prouvez que $a + b \bmod n = [(a\ mod\ n) + (b\ mod\ n)]\ mod\ n$

Réponses

1) L'inverse est 20, car $14 \times 20\ mod\ 31 = 1$. Nous pouvons l'obtenir par énumération ou alors avec la méthode d'Euclide étendu.
2) $PGDC(1540, 546) = 14 = \mathbf{11} \times 1540 - \mathbf{31} \times 546$. Les coefficients de Bézout sont donc 11 et -31.
3) $12^{27}\ mod\ 15 = (12^{16} \times 12^{8} \times 12^{2} \times 12^{1})\ mod\ 15 = (12^{16} mod\ 15 \times 12^{8} mod\ 15 \times 12^{2} mod\ 15 \times 12^{1} mod\ 15) mod\ 15 = (6 \times 6 \times 9 \times 12) mod\ 15 = 12.$
4) Posons $a + b \bmod n = x$, il existe donc un $k \in \mathbb{N}$ tel que $a + b = k \times n + x$.
   Posons $a\ mod\ n = x_a$ et $b\ mod\ n = x_b$, on a donc qu'il existe $k_a, k_b \in \mathbb{N}$ tels que $a = k_a \times n + x_a$ et $b = k_b \times n + x_b$. Donc
   $a + b = k_a \times n + x_a + k_b \times n + x_b = (k_a + k_b) \times n + (x_a + x_b)$.
   Prenons l'égalité ci-dessus modulo n, alors les multiples de n disparaissent et il nous reste que $a + b \bmod n = (x_a + x_b)\ mod\ n = [(a\ mod\ n) + (b\ mod\ n)]\ mod\ n$. □