

Mathématiques discrètes pour l'informatique

Examen du 20 mai 2010. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Question 1 : PGCD et PPCM

1. Soient deux entiers naturels non nuls a et b . Montrez que a et b sont premiers entre eux si et seulement si $PPCM(a, b) = ab$.
2. Déterminez l'ensemble des couples (a, b) d'entiers naturels non nuls vérifiant

$$2PPCM(a, b) + 3PGCD(a, b) = 159.$$

Réponse.

1. (1 point) Remarquons que l'on a toujours $PGCD(a, b) \times PPCM(a, b) = ab$. Alors

$$PPCM(a, b) = \frac{ab}{PGCD(a, b)}.$$

a et b sont premiers entre eux si et seulement si $PGCD(a, b) = 1$. Et $PGCD(a, b) = 1$ si et seulement si $PPCM(a, b) = ab$.

2. (2 points) Posons $d = PGCD(a, b)$. Alors il existe deux entiers naturels non nuls a' et b' premiers entre eux tels que

$$\begin{cases} a = da' \\ b = db' \\ PPCM(a, b) = da'b' \end{cases}$$

Alors

$$\begin{aligned} 2PPCM(a, b) + 3PGCD(a, b) &= 159 \\ \Leftrightarrow 2da'b' + 3d &= 159 \\ \Leftrightarrow d(2a'b' + 3) &= 159. \end{aligned}$$

On en déduit que $2a'b' + 3$ est un diviseur de 159. D'ailleurs, $2a'b' + 3 > 3$ alors il n'y a que deux cas possibles :

Cas 1. $2a'b' + 3 = 53$. Dans ce cas, $d = 3$, $a'b' = 25$. Comme a' et b' sont premiers entre eux, $(a', b') = (1, 25)$ ou $(25, 1)$. Il existe 2 solutions $(a, b) = (3, 75)$ ou $(75, 3)$.

Cas 2. $2a'b' + 3 = 159$. Dans ce cas, $d = 1$, $a'b' = 78$, il existe 8 solutions $(a, b) = (1, 78), (2, 39), (3, 26), (6, 13)$ ou $(13, 6), (26, 3), (39, 2), (78, 1)$.

Question 2 : Congruences

1. Déterminez l'inverse de 17 dans $\mathbb{Z}/64\mathbb{Z}$.
2. Résolvez le système suivant :

$$\begin{cases} 2x \equiv 7 \pmod{9} \\ 7x \equiv 9 \pmod{11} \end{cases}$$

Réponse.

1. (1 point) Par l'algorithme d'Euclide étendu, on obtient $64 \times 4 - 17 \times 15 = 1$. Alors l'inverse de 17 est $64 - 15 = 49$.
2. (2 points) En appliquant l'algorithme d'Euclide étendu pour les couples $(9, 2)$ et $(11, 7)$, on déduit

$$2x \equiv 7(\text{mod } 9) \Leftrightarrow x \equiv 8(\text{mod } 9)$$

et

$$7x \equiv 9(\text{mod } 11) \Leftrightarrow x \equiv 6(\text{mod } 11).$$

Alors le système original devient

$$\begin{cases} x \equiv 8(\text{mod } 9) \\ x \equiv 6(\text{mod } 11) \end{cases}$$

L'algorithme d'Euclide étendu nous donne $11 \times 5 - 9 \times 6 = 1$. Alors une solution particulière est

$$11 \times 5 \times 8 - 9 \times 6 \times 6 = 116.$$

La solution générale est donnée par $x \equiv 116(\text{mod } 99)$.

Question 3 : RSA

On considère le système cryptographique RSA avec la clé publique $(n, e) = (159, 57)$.

1. Est-ce que le couple (n, e) est une clé publique possible pour RSA ? Justifiez.
2. Quelle est la clé secrète $(\varphi(n), d)$ qui permet de décoder les messages ?
3. Quel est le cryptogramme du message $M = 125$?
4. On déchiffre $C = 70$. Quelle est la valeur du message ?

Réponse.

1. (2 points) $n = 159$ est le produit des deux nombres premiers distincts $p = 3$ et $q = 53$. L'indicatrice d'Euler $\varphi(n)$ est donnée par

$$\varphi(n) = (p - 1)(q - 1) = 104.$$

De plus, $\varphi(n) = 104$ et $e = 57$ sont premiers entre eux alors $(n, e) = (159, 57)$ est une clé publique possible pour RSA.

2. (2 points) En appliquant l'algorithme d'Euclide étendu pour le couple $(\varphi(n), e) = (104, 57)$, on obtient

$$104 \times 17 + 57 \times (-31) = 1.$$

Alors $57 \times (-31) \equiv 1(\text{mod } 104)$. Donc, $d = 104 - 31 = 73$. La clé secrète est $(\varphi(n), d) = (104, 73)$.

3. (2 points) Le message chiffré C satisfait

$$C \equiv M^e(\text{mod } n) \equiv 125^{57}(\text{mod } 159).$$

En base binaire, $57 = 2^5 + 2^4 + 2^3 + 1$.

On a

- $125 \equiv -34(\text{mod } 159)$.
- $125^2 \equiv (-34)^2 = 1156 \equiv 43(\text{mod } 159)$.
- $125^{2^2} \equiv 43^2 = 1849 \equiv 100 \equiv -59(\text{mod } 159)$.
- $125^{2^3} \equiv (-59)^2 = 3481 \equiv 142 \equiv -17(\text{mod } 159)$.
- $125^{2^4} \equiv (-17)^2 = 289 \equiv 130 \equiv -29(\text{mod } 159)$.

$$-125^{25} \equiv (-29)^2 = 841 \equiv 46 \pmod{159}.$$

Alors,

$$\begin{aligned} C &\equiv 46 \times (-29) \times (-17) \times (-34) \pmod{159} \\ &= -771052 \equiv 98 \pmod{159}. \end{aligned}$$

Donc, le message chifré C est 98.

4. (2 points) Le message original M est déterminé par

$$M \equiv C^d \pmod{n} \equiv 70^{73} \pmod{159} \equiv 70^{64} \times 70^8 \times 70^1 \equiv 28 \times 49 \times 70 \equiv 4 \pmod{159}.$$

Alors $M = 4$.

Question 4 : Séries génératrices

On considère la suite (a_n) :

$$\begin{cases} a_0 = 1 \\ a_1 = 5 \\ a_n = 5a_{n-1} - 6a_{n-2} \quad \forall n \geq 2 \end{cases}$$

1. Déterminez la forme close de la série génératrice correspondante.
2. Déterminez le terme général a_n .

Réponse.

1. (2 points) La série génératrice est définie par

$$A(x) = \sum_{n \geq 0} a_n x^n.$$

Alors

$$A(x) = a_0 + a_1 x + 5x(A(x) - a_0) - 6x^2 A(x).$$

Donc

$$A(x) = \frac{a_0 + a_1 x - 5a_0 x}{1 - 5x + 6x^2} = \frac{1}{1 - 5x + 6x^2}.$$

2. (4 points) $A(x)$ peut être décomposée en éléments simples :

$$A(x) = \frac{-2}{1 - 2x} + \frac{3}{1 - 3x}.$$

Alors

$$A(x) = -2 \sum (2x)^n + 3 \sum (3x)^n = \sum (3^{n+1} - 2^{n+1}) x^n.$$

Le terme général de la suite est $a_n = 3^{n+1} - 2^{n+1}$.