

Mathématiques discrètes pour l'informatique

Examen du 19 mai 2011. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Le barème est donné à titre indicatif.

Question 1. (3 points)

1. Soit n un nombre naturel plus grand ou égal à 2. On considère p le plus petit nombre naturel tel que p divise n et $p \geq 2$. Montrez que p est un nombre premier.
2. Montrez que l'ensemble des nombres premiers est infini.
3. Déterminez l'ensemble des couples (a, b) de nombres naturels non nuls vérifiant

$$\text{pgcd}(a, b) + \text{ppcm}(a, b) = a + b + 6.$$

Réponse. Preuves par l'absurde. Il y a 6 couples : $(2, 7), (7, 2), (3, 4), (4, 3), (6, 9), (9, 6)$.

Question 2 : Congruences (3 points)

1. Déterminez l'inverse de 30 dans $\mathbb{Z}/67\mathbb{Z}$.
2. Résolvez le système suivant :

$$\begin{cases} 30x \equiv 7 \pmod{67} \\ 11x \equiv 9 \pmod{23} \end{cases}$$

Réponse.

1. Par l'algorithme d'Euclide étendu, on obtient $67 \times 13 - 30 \times 29 = 1$. Alors l'inverse de 30 est $67 - 29 = 38$.
2. En appliquant l'algorithme d'Euclide étendu pour les couples $(67, 30)$ et $(23, 11)$, on déduit

$$30x \equiv 7 \pmod{67} \Leftrightarrow x \equiv 38 * 7 \equiv 65 \pmod{67}$$

et

$$11x \equiv 9 \pmod{23} \Leftrightarrow x \equiv 5 \pmod{23}.$$

Alors le système original devient

$$\begin{cases} x \equiv 65 \pmod{67} \\ x \equiv 5 \pmod{23} \end{cases}$$

L'algorithme d'Euclide étendu nous donne $67 \times 11 - 23 \times 32 = 1$. Alors une solution particulière est

$$67 \times 11 \times 5 - 23 \times 32 \times 65 = -44155.$$

La solution générale est donnée par $x \equiv -44155 \pmod{1541}$.

Question 3 : L'algorithme à clé publique RSA (8 points)

1. Parmi les couples $(897, 70)$, $(899, 77)$ et $(3599, 77)$, lesquels sont des clés publiques possibles pour RSA ? Justifiez.
2. Quelles sont les clés secrètes correspondantes $(\varphi(n), d)$?

3. Quels sont les cryptogrammes du message $M = 125$?
4. On déchiffre $C = 1$. Quels sont les messages correspondantes ?

Réponse.

1. $897 = 3 * 13 * 23$ alors le couple $(897, 70)$ ne peut pas être une clé publique pour RSA.
 $899 = 29 * 31$ alors $\varphi(899) = 28 * 30$ n'est pas premier avec 77 alors $(899, 77)$ ne peut pas être une clé publique pour RSA.
 $n = 3599 = 59 * 61$ est le produit des deux nombres premiers distincts $p = 59$ et $q = 61$.
L'indicatrice d'Euler $\varphi(n)$ est donnée par

$$\varphi(n) = (p-1)(q-1) = 58 * 60 = 3480.$$

De plus, $\varphi(n) = 3480$ et $e = 77$ sont premiers entre eux alors $(n, e) = (3599, 77)$ est une clé publique possible pour RSA.

2. En appliquant l'algorithme d'Euclide étendu pour le couple $(\varphi(n), e) = (3480, 77)$, on obtient

$$3480 \times 36 + 77 \times (-1627) = 1.$$

Alors $77 \times (-1627) \equiv 1 \pmod{3480}$. Donc, $d = 3480 - 1627 = 1853$. La clé secrète est $(\varphi(n), d) = (3480, 1853)$.

3. Le message chiffré C satisfait

$$C \equiv M^e \pmod{n} \equiv 125^{77} \pmod{3599}.$$

En base binaire, $77 = 64 + 8 + 4 + 1 = 2^6 + 2^3 + 2^2 + 1$.

On a

- $125^2 \equiv 1229 \pmod{3599}$.
- $125^{2^2} \equiv 1229^2 \equiv 2460 \pmod{3599}$.
- $125^{2^3} \equiv 2460^2 \equiv 1681 \pmod{3599}$.
- $125^{2^4} \equiv 1681^2 \equiv 546 \pmod{3599}$.
- $125^{2^5} \equiv 546^2 \equiv 2998 \pmod{3599}$.
- $125^{2^6} \equiv 2998^2 \equiv 1301 \pmod{3599}$.

Alors,

$$C \equiv 1301 \times 1681 \times 2460 \times 125 \equiv 2431 \pmod{3599}$$

Donc, le message chiffré C est 2431.

4. Le message original M est déterminé par

$$M \equiv C^d \pmod{n} \equiv 1^{1853} \equiv 1 \pmod{3599}.$$

Alors le message original M est 1.

Question 4 : Séries génératrices (6 points)

On considère la suite (a_n) :

$$\begin{cases} a_0 = 1 \\ a_1 = 7 \\ a_n = 7a_{n-1} - 12a_{n-2} \quad \forall n \geq 2 \end{cases}$$

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

Réponse.

1. La série génératrice est définie par

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

Alors

$$A(x) = a_0 + a_1 x + 7x(A(x) - a_0) - 12x^2 A(x).$$

Donc

$$A(x) = \frac{a_0 + a_1 x - 7a_0 x}{1 - 7x + 12x^2} = \frac{1}{1 - 7x + 12x^2}.$$

2. Le polynôme $1 - 7x + 12x^2$ admet deux racines simples $1/3$ et $1/4$:

$$1 - 7x + 12x^2 = (1 - 3x)(1 - 4x).$$

$A(x)$ peut être décomposée en éléments simples :

$$A(x) = \frac{-3}{1 - 3x} + \frac{4}{1 - 4x}.$$

Alors

$$A(x) = -3 \sum (3x)^n + 4 \sum (4x)^n = \sum (4^{n+1} - 3^{n+1}) x^n.$$

Le terme général de la suite est $a_n = 4^{n+1} - 3^{n+1}$.