Université Paris Est Créteil Val de Marne
Licences d'Informatique
2013-2014

Corrigé Contrôle continu 2 : Mathématiques discrètes pour l'informatique
(Sans documents. Les calculatrices sont autorisées.)

[3pts] **Question 1 : Congruences**

Résoudre le système de congruences suivant

$$(S_2)\begin{cases} x \equiv 5(\text{mod } 123) \\ x \equiv 5(\text{mod } 20) \end{cases}$$

Réponse. Dans ce cas il est évident que 5 est une solution particulière de (S_2), on a

$$(S_2) \Longleftrightarrow PPCM(120, 23)|(x-5).$$

Comme 123 et 20 sont premiers entre eux, $PPCM(120, 23) = 123 \times 20 = 2460$.
(S_2) est équivalent à $2460|(x-5)$, alors les solutions de (S_2) sont $x = 5 + 2460k, k \in \mathbb{Z}$.

[7pts] **Question 2 : RSA**

On considère le système cryptographique RSA avec la clé publique $(n, e) = (77, 53)$.

1. Le couple (n, e) est-il 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 $M = 25$?

Réponse.

1. *(3 points)* $n = 77$ est le produit des deux nombres premiers distincts $p = 7$ et $q = 11$. L'indicatrice d'Euler $\varphi(n)$ est donnée par

$$\varphi(n) = (p-1)(q-1) = 6 * 10 = 60.$$

De plus, $\varphi(n) = 60$ et $e = 53$ sont premiers entre eux alors $(n, e) = (77, 53)$ est une clé publique possible pour RSA.

2. *(2 points)* En appliquant l'algorithme d'Euclide étendu pour le couple $(\varphi(n), e) = (60, 53)$, on obtient

$$60 \times (-15) + 53 \times (17) = 1.$$

Alors $53 \times (17) \equiv 1(mod\ 60)$. Donc, $d = 17$. La clé secrète est $(\varphi(n), d) = (60, 17)$.

3. *(2 points)* Le message chiffré C satisfait

$$C \equiv M^e(mod\ n) \equiv 25^{53}(mod\ 77).$$

Méthode 1 : En base binaire, $53 = 1\,1\,0\,1\,0\,1_2$.

– Bit 4 : $C = 25 \times 25[77] \equiv 9[77]$, $C \equiv 9 \times 25(mod\ 77) \equiv 71(mod\ 77)$.

– Bit 3 : $C = 71 \times 71[77]$, $C \equiv 36(mod\ 77)$.

- Bit 2 : $C = 36 \times 36[77] \equiv 64[77]$, $C \equiv 64 \times 25(mod\ 77) \equiv 60(mod\ 77)$.
- Bit 1 : $C = 60 \times 60[77]$, $C \equiv 58(mod\ 77)$.
- Bit 0 : $C = 58 \times 58[77] \equiv 53[77]$, $C \equiv 53 \times 25(mod\ 77) \equiv 16(mod\ 77)$.

Donc, le message chifré C est 16.

Méthode 2 :

En base binaire, $53 = 2^5 + 2^4 + 2^2 + 1$.

Donc $25^{53} = 25^{2^5} \times 25^{2^4} \times 25^{2^2} \times 25$.

On a

- $25 \equiv 25(mod\ 77)$.
- $25^2 \equiv (25)^2 = 625 \equiv 9(mod\ 77)$.
- $25^{2^2} \equiv 9^2 = 81 \equiv 4(mod\ 77)$.
- $25^{2^3} \equiv (4)^2 = 16(mod\ 77)$.
- $25^{2^4} \equiv (16)^2 = 256 \equiv 25(mod\ 77)$.
- $25^{2^5} \equiv (25)^2 = 9(mod\ 77)$.

Alors,

$$\begin{aligned} C &\equiv 9 \times 25 \times 4 \times 25(mod\ 77) \\ &= 22500 \equiv 16(mod\ 77). \end{aligned}$$

Donc, le message chifré C est 16.