RÉCRÉATION MATHÉMATIQUES : CRYPTOGRAPHIE

Définitions

1. Soient a et $n \neq 0$ deux entiers, on note a modulo n le reste de la division entière de a par n.
2. Soient a, b et $n \neq 0$ trois entiers. On dit que a est congru à b modulo n et on note $a \equiv b$ modulo n si a modulo n est égal à b modulo n.
3. Soient a, $b \in \mathbb{Z}$. On dit que a divise b, s'il existe $q \in \mathbb{Z}$ t.q $b = aq$.
4. Soient a, $b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux si pgcd(a,b)=1.
5. Pour $n > 0$, la fonction d'Euler est définie par

$$\phi(n) = \{\text{card } a \in \mathbb{N}, 0 < a < n \mid \text{pgcd}(a, n) = 1\}$$

6. Si a et b sont premiers entre eux, il existe un entier $d < b$ t.q $ad \equiv 1$ modulo b.

Exercices

Pour la suite a, b et n sont trois entiers et $n \neq 0$. Le nombre de ♣ dénote la difficulté de l'exercice.

1. ♣ Montrez que $a \equiv b$ modulo n si et seulement si n divise $a - b$ (utilisez la définition 2).
2. ♣ Montrez que si $a \equiv b$ modulo n et si $b < n$ alors a modulo $n = b$ (utilisez l'exercice précédent).
3. ♣ Montrez que a et b sont premiers entre eux si et seulement si les seuls diviseurs de a et b sont 1 et -1 (utilisez la définition 4).
4. ♣ Soit p un nombre premier, montrez que tout entier j, t.q $0 < j < p$, est premier avec p.
5. ♣ Soit p un nombre premier, démontrez que les seuls entiers non premiers avec p et strictement plus grand que p sont les multiples de p.
6. ♣♣ Soit p un nombre premier et k un entier positif, démontrez que $\phi(p^k) = p^k - p^{k-1}$.
7. ♣♣ Soit m et n deux entiers premiers entre eux, démontrez que $\phi(mn) = \phi(m)\phi(n)$.
8. ♣ En utilisant le résultat de l'exercice 1, montrez que si $a \equiv b$ modulo n, alors pour tout $c \in \mathbb{Z}$:
- . $a + c \equiv b + c$ modulo n,
- . $ac \equiv bc$ modulo n,
- . si $b \equiv c$ modulo n, alors $a \equiv c$ modulo n.

9. ♣♣♣ Il s'agit dans cet exercice de démontrer que pour tout entier a premier avec n, $a^{\phi(n)} \equiv 1$ modulo n.
- . Soient α et β deux entiers premiers avec n, montrez que $\alpha\beta$ est premier avec n.
- . Notons $b_1, \ldots, b_{\phi(n)}$ les $\phi(n)$ entiers strictement inférieurs à n qui sont premiers avec n. Déduisez de la question précédente que $\forall i = 1 \ldots \phi(n)$, ab_i modulo n est premier avec n.
- . En déduire que $\prod_{i=1}^{\phi(n)} ab_i \equiv \prod_{i=1}^{\phi(n)} b_i$ modulo n.
- . Conclure.

10. ♣♣♣ On se propose dans cet exercice de démontrer que le déchiffrement RSA fonctionne même si le message m n'est pas premier avec n.
- . Montrez que si m n'est pas premier avec n alors m est un multiple de p ou q.
- . La démonstration étant identique que m soit un multiple de p ou de q, on supposera pour la suite que c'est un multiple de p. Que vaut $m^{(q-1)}$ modulo q ?
- . En déduire qu'il existe un entier j t.q $m^{k\phi(n)+1} = m + mjq$.
- . Conclure.

11. ♣♣ Montrez que dans le système RSA, la probabilité d'engendrer un message m non premier avec n est bornée par $1/p + 1/q$. Est-il gênant d'engendrer un tel message ?
11. ♣ Démontrez qu'un entier $j > 0$ se décompose sur $\lfloor \log_2 j \rfloor + 1$ symboles en base 2.

Département d'Informatique, Université de Toulon-Var

Date: Janvier 2004.