

Mathématiques discrètes. C6 - Théorie des nombres.

Application à la cryptographie.

31 mars 2010

1 Théorèmes de congruences.

Petit théorème de Fermat. Soit p un nombre premier. Pour tout entier a , on a la congruence

$$a^p \equiv a \pmod{p}.$$

Cas 1 : Si a est un multiple de p , a^p l'est aussi, alors OK.

Cas 2 : Si a n'est pas multiple de p , a et p sont premiers entre eux.

$$\begin{aligned} & a^p \equiv a \pmod{p} \\ \Leftrightarrow & p \mid (a^p - a) \\ \Leftrightarrow & p \mid a(a^{p-1} - 1) \\ \Leftrightarrow & p \mid (a^{p-1} - 1) \quad \text{lemme de Gauss} \\ \Leftrightarrow & a^{p-1} \equiv 1 \pmod{p}. \end{aligned}$$

Dans ce cas, le théorème est équivalent au corollaire suivant.

Corollaire 1. Soit p un nombre premier. Pour tout entier a premier avec p , on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

Idées de la preuve. Dans $\mathbb{Z}/p\mathbb{Z}$, les $p - 1$ nombres

$$a, 2a, \dots, (p-1)a$$

sont non-nuls (ne sont pas multiples de p) et deux à deux distincts (modulo p).

Alors l'ensemble de ces $(p-1)$ nombres coïncide à l'ensemble $\{1, 2, \dots, (p-1)\}$ dans $\mathbb{Z}/p\mathbb{Z}$. En particulier, on a

$$a \times 2a \times \dots (p-1)a = 1 \times 2 \times \dots (p-1) \text{ dans } \mathbb{Z}/p\mathbb{Z}$$

c.a.d.,

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

D'où la conclusion.

Corollaire 2. Soit $n = pq$ où p et q sont deux nombres premiers distincts. Pour tout a premier avec n , on a

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

Preuve. a est premier avec $n = pq$ alors a est aussi premier avec p et q . D'après le petit théorème de Fermat, on a

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{(p-1)(q-1)} \equiv 1 \pmod{p},$$

et

$$a^{p-1} \equiv 1 \pmod{q} \Rightarrow a^{(p-1)(q-1)} \equiv 1 \pmod{q}.$$

De plus, p et q sont premiers entre eux (car il s'agit de deux nombres premiers distincts) alors

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Définition. (Indicatrice d'Euler) Soit n un entier positif. L'indicatrice d'Euler de n , notée $\varphi(n)$, est défini par le nombre des entiers k entre 1 et n premiers avec n :

$$\begin{cases} 1 \leq k \leq n \\ \text{PGCD}(k, n) = 1. \end{cases}$$

Exemple. $\varphi(8) = 4$.

Théorème. Soit n un entier positif. L'indicatrice d'Euler de n est donnée par

$$\varphi(n) = n \prod_{p \in \mathcal{P}, p|n} \left(1 - \frac{1}{p}\right).$$

Exemple. Pour $n = p$ un nombre premier, $\varphi(p) = p - 1$.

Pour $n = p^k$, une puissance d'un nombre premier p , $\varphi(p^k) = (p - 1)p^{k-1}$.

Pour $n = pq$, le produit de deux nombres premiers distincts, $\varphi(pq) = (p - 1)(q - 1)$.

Trouver $\varphi(20)$.

Par définition, on considère tous les entiers entre 1 et 20 :

$$\{1, 2, 3, 4, 5 \dots 20\}$$

Parmi ces nombres, les suivants sont premiers avec 20

$$\{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Il y en a 8, alors $\varphi(20) = 8$.

Par le théorème : On décompose 20 en facteurs premiers $20 = 2^2 \cdot 5$. Alors

$$\varphi(20) = 20 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 20 \times \frac{1}{2} \times \frac{4}{5} = 8.$$

Théorème d'Euler. Soit n un entier positif, Pour tout a premier avec n , on a la congruence

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Preuve. Similaire à la preuve du corollaire 1.

Remarques. Si on applique le théorème d'Euler pour $n = p$ et $n = pq$, on retrouve les corollaires 1 et 2 du petit théorème de Fermat.

2 Application à la cryptographie. Algorithme à clé publique RSA.

Qu'est-ce que c'est la cryptographie ?

En grec, *kryptos* = caché et *graphein* = écriture. La cryptographie est donc l'art de coder un message pour le rendre illisible par toute autre personne que son destinataire.

Exemple. Alice transmet un message chiffré ♥ à Bernard en évitant que Charles peut le traduire.

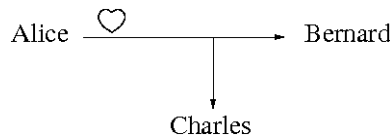


FIG. 1 – Premier exemple.

L'idée de base de l'algorithme à clé publique RSA :

1. Bernard émet une clé publique que reçoit Alice et aussi Charles.
2. Avec cette clé, Alice peut chiffrer un message qu'elle émet. L'algorithme doit assurer que même si Charles intercepte le message chiffré de cette manière, il ne peut pas le déchiffrer.
3. Bernard peut déchiffrer le message codé avec une clé secrète que personne d'autre ne la connaît.

Théorème RSA. Soient p et q deux nombres premiers distincts et $n = pq$. Pour tout entier positif e premier avec $\varphi(n) = (p-1)(q-1)$, il existe un entier positif d tel que

$$ed \equiv 1 \pmod{\varphi(n)}$$

et tel que pour tout entier a premier avec n , on a

$$a^{ed} \equiv a \pmod{n}.$$

Preuve. En appliquant l'algorithme d'Euclide étendu au couple de deux entiers premiers entre eux $(e, \varphi(n))$, on obtient l'entier d t.q. $ed \equiv 1 \pmod{\varphi(n)}$, c.a.d., $ed - 1 = k\varphi(n), k \in \mathbb{N}$.

D'après le corollaire 2 du petit théorème de Fermat (ou le théorème d'Euler), pour tout a premier avec n , on a

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Alors

$$a^{ed-1} = a^{k\varphi(n)} = (a^{\varphi(n)})^k \equiv 1^k = 1 \pmod{n}.$$

En multipliant par a , on obtient

$$a^{ed} \equiv a \pmod{n}.$$

Remarque. Même si a n'est pas premier avec n , on a toujours la congruence

$$a^{ed} \equiv a \pmod{n}.$$

Algorithme à clé publique RSA.

1. Bernard choisit deux nombres premiers suffisamment grands p et q . Il calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$. Il choisit e et calcule ensuite le d t.q.

$$ed \equiv 1 \pmod{\varphi(n)}.$$

2. Bernard émet publiquement la clé (n, e) . D'où, ce couple s'appelle *la clé publique*.
3. Alice décompose l'information à transmettre en un ou plusieurs nombres a_1, a_2, \dots inférieurs à n . Elle calcule les restes r_1, r_2, \dots des divisions euclidiennes de ces nombres a_1^e, a_2^e, \dots par n . On a

$$r_i \equiv a_i^e \pmod{n}.$$

Alice émet ces restes r_1, r_2, \dots vers Bernard.

4. Bernard peut déchiffrer, c.a.d., retrouver les nombres a_1, a_2, \dots en calculant les restes des divisions euclidiennes de r_1^d, r_2^d, \dots par n . Car

$$r_i^d = (a_i^e)^d = a_i^{ed} \equiv a_i \pmod{n}.$$

Même si Charles a réussi à intercepter les nombres r_1, r_2, \dots envoyés par Alice, il ne sait pas effectuer le décodage comme il ne connaît pas $\varphi(n)$ et l'entier d . Et on appelle le couple $(\varphi(n), d)$ *la clé secrète* du système RSA.

Remarque. Le système RSA repose sur le fait que l'on ne sait décomposer rapidement un grand entier en facteurs premiers. D'où, il est impossible pour Charles de déterminer le couple (p, q) t.q. $n = pq$ et de déterminer la clé secrète $(\varphi(n), d)$.

Dans la pratique, il faut choisir des nombres n les plus grands possibles. Longueurs de clés recommandées :

- pour un usage individuel, 768 bits soit l'équivalent de 231 chiffres décimaux.
- pour des entreprises, 1024 bits soit l'équivalent de 308 chiffres décimaux ;
ou 2048 bits soit l'équivalent de 616 chiffres décimaux.

Le FBI américain utiliserait une clé de 4096 bits.

Exemple. Pour $p = 11$, $q = 19$ et $e = 7$, déterminer les clés publiques et secrètes.

1. On a

$$n = pq = 209 \quad \varphi(n) = (p-1)(q-1) = 180.$$

La clé publique est le couple $(n, e) = (209, 7)$.

2. On effectue l'algorithme d'Euclide étendu pour le couple $(\varphi(n), e) = (180, 7)$:

a	b	q	r	u	u'	v	v'
180	7	25	5	1	0	0	1
7	5	1	2	0	1	1	-25
5	2	2	1	1	-1	-25	26
2	1	2	0	-1	3	26	-77
1	0			3		-77	

On obtient $180 \times 3 + 7 \times (-77) = 1$, donc $7 \times (-77) \equiv 1 \pmod{180}$.
L'entier positif d est donné par

$$d = -77 + 180 = 103.$$

La clé secrète est $(\varphi(n), d) = (180, 103)$.

Si Alice veut envoyer le message $a = 99$, elle utilise la clé publique (n, e) pour le chiffrer :

$$r \equiv a^e \equiv 99^7 \pmod{209}.$$

Pour ce fait, elle peut décomposer l'exposant 7 en somme des puissances de 2 : $7 = 2^2 + 2 + 1$ et donc

$$99^7 = 99^{2^2} \times 99^2 \times 99$$

$$99^2 = 9801 \equiv 187 \equiv -22 \pmod{209}$$

$$99^{2^2} \equiv (99^2)^2 \equiv (-22)^2 \equiv 66 \pmod{209}$$

Alors

$$99^7 \equiv 66 \times (-22) \times 99 \equiv 44 \pmod{209}$$

Le message chiffré est $r = 44$.

Bernard peut déchiffrer ce message en calculant $r^d = 44^{103} \pmod{209}$. On décompose l'exposant 103 en $103 = 2^6 + 2^5 + 2^2 + 2 + 1$.

$$44^2 \equiv 55 \pmod{209}$$

$$44^{2^2} \equiv 55^2 \equiv 99 \pmod{209}$$

$$44^{2^3} \equiv 99^2 \equiv -22 \pmod{209}$$

$$44^{2^4} \equiv (-22)^2 \equiv 66 \pmod{209}$$

$$44^{2^5} \equiv 66^2 \equiv 176 \equiv -33 \pmod{209}$$

$$44^{2^6} \equiv (-33)^2 \equiv 44 \pmod{209}$$

Alors

$$44^{103} \equiv 44^{2^6} \times 44^{2^5} \times 44^{2^2} \times 44^2 \times 44 \equiv 44 \times (-33) \times 99 \times 55 \times 44 = 99 \pmod{209}.$$

Bernard retrouve effectivement le message original 99 que Alice veut lui transmettre.