EUCLIDE et RSA

1 Cours

Soient a et b deux entiers non-nuls. Si $a = p_2^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ et $b = p_1^{f_1} p_2^{f_2} \cdots q_n^{f_n}$ alors $pgcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)}$. La factorisation des entiers est un problème difficile sur lequel repose la sécurité des certains systèmes cryptologiques.

L'algorithme d'Euclide est une méthode rapide pour trouver $pgcd(a,b)$. Si a ou b sont nuls le résultat est connu sans calcul. Quitte à échanger a et b on peut supposer $a \geq b$. On pose $u_0 = 1$, $v_0 = 0$ et $d_0 = a$ et on écrit :

$$u_0 \cdot a + v_0 \cdot b = d_0. \tag{0}$$

On pose ensuite $u_1 = 0$, $v_1 = 1$ et $d_1 = b$ et on vérifie :

$$u_1 \cdot a + v_1 \cdot b = d_1. \tag{1}$$

On pose $i = 1$. Tant que $d_i \neq 0$, on appelle q_i le quotient et le reste de la division euclidienne de d_{i-1} par d_i. On appelle $(i+1)$ l'équation obtenue par la formule $(i-1) - q_i \cdot (i)$, autrement dit on obtient une équation correcte en posant $u_{i+1} = u_{i-1} - q_i u_i$, $u_{i+1} = u_{i-1} - q_i u_i$ alors que $d_{i+1} = d_{i-1} - q_i d_i$ est le reste de d_{i-1} par d_i :

$$u_i \cdot a + v_i \cdot b = d_i. \tag{i}$$

On appelle n la dernière valeur de i où d_i est non-nul, et alors $d_{n+1} = 0$.

Théorème 1. $d_n = pgcd(a,b)$.

Démonstration. Pour tout i, comme $\text{pgcd}(a,b)$ divise a il divise aussi $u_i a$. de même $\text{pgcd}(a,b)$ divise $v_i b$, et alors $\text{pgcd}(a,b)$ divise $u_i a + v_i b = d_i$. En particulier pour $i = n$, $\text{pgcd}(a,b)$ divise d_n.

Réciproquement, montrons que d_n divise $pgcd(a,b)$, ce qui finira la preuve. Puisque $d_{n+1} = 0$ et $d_{n-1} = q_{n+1} d_n + d_{n+1}$, $d_n \mid d_{n-1}$. Ensuite, puisque $d_{n-2} = q_{n-1} d_{n-1} + d_n$, d_n divise d_{n-2}.

Montrons par récurrence sur $0 \leq k \leq n$ la proposition $P(k)$: d_n divise les entiers $d_{n-1}, \ldots, d_{n-k}$.

initialisation : $k = 1$ et $k = 2$ déjà montré.

hérédité : Supposons le résultat vrai pour un entier k inférieur à n et montrons le résultat pour $k+1$. Par l'hypothèse de récurrence, d_n divise $d_{n-(k-1)}$

et d_{n-k}. Puisque $d_{n-(k+1)} = q_{n-k}d_{n-k} + d_{n-(k-1)}$ on déduit que d_n divise $d_{n-(k+1)}$.

En particulier d_n divise $d_0 = a$ et $d_1 = b$, donc il divise $pgcd(a, b)$. □

Remarque 1. Si on combine les équations sans respecter l'algorithme alors il reste vrai que $pgcd(a, b)$ divise d_n. Pour la réciproque, il reste vrai que d_n divise d_{n-1}, mais on n'a pas forcément que d_n divise les autres d_i donc on ne peut pas remonter à $d_1 = b$ et $d_0 = a$.

Exemple 1. Prenons l'exemple de $a = 60068$ et $b = 40016$. Au début on suit l'algorithme et on pose :

$$1 \cdot a + 0 \cdot b = 60068 \tag{0}$$

$$0 \cdot a + 1 \cdot b = 40024 \tag{1}$$

On voit que $2a$ est proche de $3b$ et alors on pose $(2) = 2(0) - 3(1)$ ce qui ne correspond pas à l'algorithme mais donne une équation correcte :

$$2 \cdot a - 3 \cdot b = 64 \tag{2}$$

On reprend l'algorithme en faisant la division euclidienne de $d_1 = 40024$ par $d_2 = 64$ et on trouve $d_1 = 625 \cdot d_2 + 24$. Donc on pose $(3) = (1) - 625 \cdot (2)$:

$$-1250 \cdot a + 1876 \cdot b = 24 \tag{3}$$

Puis, comme $d_2 = 2 \cdot d_3 + 16$ on pose $(4) = (2) - 2 \cdot (3)$; comme $d_3 = 1 \cdot d_4 + 8$ on pose $(5) = (3) - (4)$; comme $d_4 = 2 \cdot d_3$ on pose $(6) = (4) - 2 \cdot (5)$:

$$2502 \cdot a - 3755 \cdot b = 16 \tag{4}$$

$$-3752 \cdot a + 5631 \cdot b = 8 \tag{5}$$

$$10006 \cdot a - 15017 \cdot b = 0. \tag{6}$$

Le dernier reste non-nul est $d_5 = 8$ alors que $a = 2^2 \cdot 15017$ et $b = 2^3 \cdot 5003$ donc $pgcd(a, b) = 4$.

Une conséquence directe de l'Euclide est un théorème de Bezout :

Théorème 2 (Bezout). Pour toute paire d'entiers non-nuls a et b il exists des entiers relatifs u et v tels que $ua + vb = pgcd(a, b)$. De plus, si a est un reste modulo un entier non-nul n tel que $pgcd(a, n) = 1$, alors il existe un unique entier $u \in [1, n - 1]$ tel que $ua \equiv 1 \pmod{n}$.

Remarque 2. Les coefficients de Bezout, u et v, ne sont pas uniques dans $\mathbb{Z}$ car on peut remplacer la paire (u, v) par $(u + a, v - b)$. L'inverse u n'est pas unique dans $\mathbb{Z}$ mais il l'est dans $[1, n - 1]$.

Démonstration. La correction de l'algorithme d'Euclide implique que $u_n a + v_n b = pgcd(a, b)$. Pour la deuxième partie du théorème, on applique la première partie pour $b = n$: $ua + vn = 1$. Alors $1 = ua + vn \equiv ua \pmod{n}$.

Si (u, v) est une paire de coefficients, quitte à remplacer (u, v) par $(u+n, v-a)$ autant de fois que néessaire, on peut amener u dans l'intervalle $[1, n]$. Il n'est clairement pas n.

Si u et u' sont deux entiers de $[1, n-1]$ tels que $au \equiv au' \pmod{n}$, alors n divise $a(u-u')$. Comme $\text{pgcd}(a, n) = 1$, n divise $u-u'$. or, $|u-u'| \leq |(n-1)-1| = n-2$, donc $u - u' = 0$. □

Définition 1. Un entier n dans l'intervalle $[1, n-1]$ tel que $ua \equiv 1 \pmod{n}$ est appellé inverse d'a modulo n. On note $\Phi(n)$ l'ensemble des restes relativelent premiers avec n : $\Phi(n) = \{a \in [1, n] \mid pgcd(a, n) = 1\}$. On appelle indicatrice d'Euler le cardinal $\varphi(n) = \text{Card}(\varphi(n))$.

Si on connait la factorisation d'un entier n on peut calculer $\varphi(n)$, grâce à la formule suivante.

Théorème 3. Si $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ alors

$$\varphi(n) = (p_1^{e_1-1}(p_1 - 1)) \cdots (p_k^{e_k-1}(p_k - 1)).$$

Démonstration. Prenons d'abord le cas où $n = p^e$ pour un premier p. Parmi les entiers de l'intervalle $[1, p^e]$ les seuls qui ne sont pas relativement premiers avec p^e sont les multiples de p, donc les entiers de la forme px avec $x \in [1, p^{e-1} - 1]$. On a alors $\text{Card}(\Phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

Prenons maintenant le cas général. Pour cela on montre que, si m et n sont deux entiers tels que $pgcd(m, n) = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$. Si on applique la formule à $m = p_1^{e_1}$ et $n = p_2^{e_2}$ alors on a $\varphi(p1^{e_1} p_2^{e_2}) = p_1^{e_1-1} p_2^{e_2-1}(p_1 - 1)(p_2 - 1)$. On applique ensuite la formule à $m = p_1^{e_1} p_2^{e_2}$ et $n = p_3^{e_3}$ pour obtenir $\varphi(p_1^{e_1} p_2^{e_2} p_3^{e_3} = p_1^{e_1-1} p_2^{e_2-1} p_3^{e_3-1}(p_1-1)(p_2-1)(p_3-1)$. Par récurrence on obtient la formule pour tout entier.

Revenons à la preuve de $\varphi(mn) = \varphi(m)\varphi(n)$ quand $pgcd(m, n) = 1$. On considère l'application $f : [0, mn-1] \to [0, m-1] \times [0, n-1]$, $x \mapsto (x \bmod m, x \bmod n)$. Si x et y sont deux éléments de $[0, mn-1]$ tels que $f(x) = f(y)$ alors $m \mid (x-y)$ et $n \mid (x-y)$. Comme $pgcd(m, n) = 1$ cela implique que mn divise $(x-y)$. Or, $x, y \in [0, mn-1]$ donc $|x-y| < mn$ et alors $x - y = 0$. Puisque le domaine et le codomaine de f on le même cardianl, $textCard([0, mn-1]) = mn = \text{Card}([0, m-1]) \cdot \text{Card}([n-1])$, tout élément de $[0, m-1] \times [0, n-1]$ est l'image d'un unique élément de $[0, mn-1]$.

Puisque $pgcd(m, n) = 1$, un élément de $a \in [1, mn]$ est relativement premier avec mn si et seulement s'il est premier avec m ET avec N, ou de manière équivalente, si $(a \bmod m) \in \Phi(m)$ et $(a \bmod n) \in \Phi(n)$. On obtient donc $\text{Card}(\Phi(mn)) = \text{Card}(\Phi(m)) \cdot \text{Card}(\Phi(n))$, soit $\varphi(mn) = \varphi(m)\varphi(n)$. □

L'indicatrice d'Euler apparaît dans un résultat qui généralise le petit théorème de Fermat.

Théorème 4 (Euler). Si n est un entier non-nul et $a \in [1, n-1]$ est tel que $pgcd(a, n) = 1$ alors

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

En particulier, pour tout premier p et tout entier relatif a on a :

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

Démonstration. L'application $f : \Phi(n) \to \Phi(n)$, $x \mapsto ax$ a comme inverse l'application $g : \Phi(n) \to \Phi(n)$, $x \mapsto ux$ où u est l'inverse de a modulo n. Ainsi f ne fait que changer l'ordre des éléments de $\Phi(n)$, elle ne change pas le produit :

$$\prod_{x \in \Phi(n)} x = \prod_{x \in \Phi(n)} f(x).$$

On pose $v = \prod_{x \in \Phi(n)} x$. On calcule :

$$\prod_{x \in \Phi(n)} f(x) = \prod_{x \in \Phi(n)} (ax) = a^{\varphi(n)} \prod_{x \in \Phi(n)} x = a^{\varphi(n)} v.$$

Or cette dernière quantité est congruente à v :

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

Comme produit d'éléments relativement premiers à n, v est relativement premier à n donc il existe $w \in [1, n-1]$ tel que $vw \equiv 1 \pmod{n}$. Alors $a^{\varphi(n)} \equiv a^{\varphi(n)} vw \equiv vw \equiv 1 \pmod{n}$.

Si $n = p$ est premier alors $\varphi(p) = p - 1$ et pour $a \not\equiv 0 \pmod{p}$ on a $a^{p-1} \equiv 1 \pmod{p}$. En multipliant par a on a $a^p \equiv a \pmod{p}$. Si $a \equiv 0 \pmod{p}$, ou de manière équivalent p divise a, alors p divise aussi $a^p - a$, soit $a^p \equiv a \pmod{p}$. □

On obtient un résultat présent sur les manuscrits d'Euler.

Théorème 5. Soit n un entier non-nul dont tous les facteurs premiers sont congruents à 2 modulo 3. Soit u l'inverse de 3 modulo $\varphi(n)$. Alors l'application

$$\begin{array}{rccc} f : & \Phi(n) & \to & \Phi(n) \\ & x & \mapsto & x^3 \end{array}$$

a comme inverse l'application

$$\begin{array}{rccc} g : & \Phi(n) & \to & \Phi(n) \\ & x & \mapsto & x^u. \end{array}$$

Démonstration. Notons d'abord que, si $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ alors, pour $i = 1, 2, \ldots, k$, $\varphi(p_i^{e_i)=p_i^{e_i-1}(p_i-1)}$ n'est pas divisible par 3. donc il existe un inverse de 3 modulo $\varphi(n)$.

Comme u est l'inverse de a modulo $\varphi(n)$, il existe un entier k tel que $au = 1 + k\varphi(n)$. Pour tout $x \in [1, n-1]$, grâce au théorème d'Eucler, on a :

$$f(g(x)) = g(f(x)) = x^{3u} = x^{1-k\varphi(n)} = x \cdot (x^{\varphi(n)})^{-k} \equiv x \cdot 1 \equiv x \pmod{n}.$$

□

Remarque 3 (RSA). Le système cryptologique RSA repose sur le théorème précédent. Le destinataire d'un message chiffré choisit deux premiers p et q et rend publique l'entier $n = pq$. Ensuite il calcule $\varphi(n) = (p-1)(q-1)$, qu'il garde secret. Il calcule l'inverse u de 3 par rapport à $\varphi(n)$ et le garde secret.

Pour envoyer un message on le coupe en groupes de quelques lettres et on transforme les lettres en nombres, par exemple a=0, b=1, etc. Le problème devient de transmettre un entier $m \in [1, n-1]$ tel que $pgcd(m, n) = 1$. Pour chiffrer le message on calcule $c := f(m) = m^3 \pmod{n}$, ce qui est possible en connaissant seulement n.

Le destinataire du message chiffré c, calcule $g(c) = g^u$, ce qui lui seul peut faire car il connait u.

Notons que l'exposant du chiffrement, $e = 3$, était le même pour tous les utilisateurs de RSA dans les années 1980. Aujourd'hui, une grande partie des implantations de RSA, par exemple sur les cartes bancaires utilisent $e = 2^16 - 1 = 65535$. Faites les modifications nécessaires dans le théorème précédent pour utiliser cette valeur de e. Notons aussi que si $\text{pgcd}(m, n)$ n'est pas 1, $(m^3)^u$ est tout de même égal au message m.

Le système RSA est utilisé par toutes les cartes bancaires mais il ourrait devenir caduque si Des avancées récentes sur l'ordinateur quantique se confirment.

2 Exercices

Exercice 1. Résoudre l'équation $(2n + 8, 3n + 15) = 6$.

Solution 1. Pour tout $n \in \mathbb{Z}$ on pose $a = 2n + 8$ et $b = 3n + 15$. L'idée est de montrer que $\text{pgcd}(a, b)$ divise un entier petit pour resteindre l'ensemble des possibilités.

Comme $3a$ et $2b$ sont proches, on écrit :

$$3 \cdot a - 2 \cdot b = -6.$$

L'équation montre que, pour tout n, $\text{pgcd}(a,b)$ divise 6 donc appartient à l'ensemble $\{1,2,3,6\}$.

Il reste à trouver des conditions équivalentes pour que 6 divise à la fois $2n+8$ et $3n+15$. D'une part, 6 divise $2n+8=2(n+4)$ si et seulement 3 divise $n+4$ ce qui équivaut à $n \equiv 2 \pmod 3$. D'autre part, 6 divise $3n+15=3(n+5)$ si et seulement si 2 divise $n+5$ ce qui équivaut à $n \equiv 1 \pmod 2$. La conjonction des deux conditions est équivalente à $n \equiv 5 \pmod 6$.

Exercice 2. Soit $n \geq 2$ un entier. Trouver le pgcd et les coefficients de Bézout correspondants de a) $n-1$ et $n+1$ puis de b) n^2+1 et n^3-n.

Solution 2. a) Pour tout n entier relatif on pose $a=n-1$ et $b=n+1$. On cherche à borner les possibilités pour $\text{pgcd}(a,b)$ et pour cela on cherche une équation comme dans l'algorithme d'Euclide :

$$(-1)\cdot a + 1 \cdot b = 2. \qquad (*)$$

Si n est impair a et b sont pairs donc $\text{pgcd}(a,b)=2$ et alors (*) est une relation de Bezout.

Si n est pair alors on note $k=n/2$ et on écrit une autre équation :

$$(-(k+1))\cdot a + k\cdot b = -(k+1)(2k-1)+k(2k+1) = -2k^2-k+1+2k^2+k = 1. \qquad (**)$$

Comme, a et b sont impairs, (**) est une équation de Bezout.

b) On pose $a=n^2+1$ et $b=n^3-n$. On commence à écrire une équation comme dans l'algorithme d'Euclide :

$$1\cdot a + 0 \cdot b = n^2+1. \qquad (0)$$

On remarque que a/b est proche de $2/n$ et on écrit une équation :

$$n\cdot a + (-1)\cdot b = n^3+n-n^3+n = 2n. \qquad (1)$$

On continue avec l'équation $(2) := 2(0) - n(1)$:

$$(2-n^2)\cdot a + n\cdot b = 2(n^2+1) - n(2n) = 2. \qquad (2)$$

Si n est impair alors (2) est une équation de Bezout. Si n est pair alors $\frac{1}{2}(2)$ est une équation de Bezout :

$$(\frac{2-n^2}{2})\cdot a + \frac{n}{2}\cdot b = 2(n^2+1) - n(2n) = 2. \qquad (2')$$