RSA - bases mathématiques

Jang SCHILTZ

Centre Universitaire de Luxembourg
Séminaire de Mathématiques
162A, avenue de la Faïencerie
L-1511 Luxembourg
Luxembourg
E-mail:schiltzj@cu.lu

1 Divisibilité

Définition 1.1 *Soient a et b des entiers. On dit que a divise b et on note $a|b$ s'il existe un entier c tel que $b = ac$. On dit alors que a est un diviseur de b, ou que b est divisible par a.*

Exemple 1.2

1. Comme $24 = 2 \cdot 12$ et $24 = 3 \cdot 8$, $2|24, 3|24, 8|24$ et $12|24$. De plus, $24 = (-2)(-12)$, donc $-2|24$ et $-12|24$.
2. Aucun entier non nul n'est divisible par 0. Si $a \neq 0$, il ne peut exister d'entier c tel que $a = c \cdot 0$. Par contre $0|0$, comme $0 = 0 \cdot c$, pour tout entier c.
3. Tout entier a divise 0, parce que $0 = 0 \cdot a$ pour tout entier a.
4. Les seuls diviseurs positifs de 5 sont 1 et 5.

Tout nombre positif a admet a et 1 comme diviseurs. Certains nombres n'en ont pas d'autres.

Définition 1.3 *Un nombre entier positif $p > 1$ est appelé nombre premier si ses seuls diviseurs sont 1 et p. Un nombre non premier est dit nombre composé.*

Les propriétés de base de la divisibilité sont les suivantes:

Proposition 1.4 *Soient a, b, c, x et y des entiers.*

1. *Si $a|b$ et $x|y$, alors $ax|by$.*
2. *Si $a|b$ et $b|c$, alors $a|c$.*
3. *Si $a|b$ et $b \neq 0$, alors, $|a| \leq |b|$.*
4. *Si $a|b$ et $a|c$, alors $a|bx + cy$.*

Théorème 1.5 *Soient deux entiers a et b, tel que $b \neq 0$. Alors, il existe des entiers q et r uniques, tels que*

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

Le nombre q est appelé le quotient de a par b et r le reste.

Exemple 1.6

1. Soient $a = 37$ et $b = 15$. Comme $37 = 2 \cdot 15 + 7$, le quotient de 37 par 15 vaut 2 et le reste 7.

2. Si $a = 37$ et $b = -15$, alors $37 = (-2)(-15) + 7$ implique que le quotient est -2 et le reste 7.

3. Si $a = -37$ et $b = 15$, alors $-37 = -2 \cdot 15 - 7 = -3 \cdot 15 + 8$. Le quotient de -37 par 15 vaut -3 et le reste 8, comme le reste doit être positif.

Définition 1.7 *Soient a et b deux entiers. On appelle plus grand commun diviseur de a et de b et on note* $\text{pgcd}\,(\text{a}, \text{b})$*, le plus grand entier qui est à la fois diviseur de a et diviseur de b.*

Proposition 1.8 *Soient a, b et n des entiers. Il existe des entiers x et y tels que $ax+by = n$ si et seulement si n est un multiple de* $\text{pgcd}\,(\text{a}, \text{b})$*. En particulier, il existe des entiers x et y tels que $ax + by =$* $\text{pgcd}\,(\text{a}, \text{b})$*.*

Exemple 1.9
Comme 3 et 4 n'ont pas de diviseurs communs supérieurs à 1, l'équation $3x + 4y = 123$ admet une solution.

Pour trouver les entiers x et y en pratique, on utilise l'algorithme d'Euclide étendu.

Définition 1.10 *On dit que deux entiers a et b sont premiers entre eux si et seulement si* $\text{pgcd}\,(\text{a}, \text{b}) = 1$*.*

Théorème 1.11 (Bezout) *Deux nombres a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $ua + vb = 1$.*

2 Arithmétique modulaire

Définition 2.1 *Si a, b et n sont des entiers, on dit que a est congru à b modulo n et on note $a \equiv b \pmod{n}$ si $n|a - b$. On dit aussi que b est un résidu de a modulo n, ou un reste de a modulo n. La relation ainsi définie est appelée congruence modulo n.*

Exemple 2.2

1. Comme $9 = 23 - 14$, la définition ci-dessus implique que $23 \equiv 14 \pmod{9}$. En fait, n'importe quels deux nombres de l'ensemble $\{..., -4, 5, 14, 23, ...\}$ sont congrus modulo 9.

2. La congruence $a \equiv b \pmod{1}$ est exacte pour tous entiers a et b.

3. Il est évident que $a \equiv b \pmod{n}$ si et seulement si $a \equiv b \pmod{(-n)}$. Pour cette raison, on ne considère que des modules positifs.

Proposition 2.3 *Si a, b, c et n sont des entiers, alors*

1. $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n}$, *si et seulement si* $b \equiv a \pmod{n}$.
3. *Si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$, *alors* $a \equiv c \pmod{n}$.

Ces trois propriétés, appelées réflexivité, symétrie et transitivité impliquent que la congruence est une relation d'équivalence. La classe d'équivalence d'un entier a pour cette relation, c'est-à-dire l'ensemble des entiers b congrus à a modulo n est la classe de congruence de a modulo n. Il existe n classes d'équivalence distinctes de la congruence modulo n. On les représente par les nombres $0, 1, ..., n-1$ et on désigne l'ensemble de ces classes de congruence par

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}.$$

La proposition suivante donne les propríétés arithmétiques élémentaires des congruences.

Proposition 2.4 *Si a, b, c, d et n sont des entiers, alors*

1. *Si* $a \equiv b \pmod{n}$, *alors* $ac \equiv bc \pmod{n}$, *pour tout entier* c.
2. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$, *alors* $a + c \equiv b + d \pmod{n}$.
3. *Si* $a \equiv b \pmod{n}$ *et* $c \equiv d \pmod{n}$, *alors* $ac \equiv bd \pmod{n}$.
4. *Si* $a \equiv b \pmod{n}$, *alors* $a^k \equiv b^k \pmod{n}$, *pour tout entier positif* k.

Exemple 2.5

1. Comme $16 \equiv -1 \pmod{17}$, $16^2 \equiv 256 \equiv 1 \pmod{17}$.
2. Calculons $2^{4k} \pmod{5}$. Comme $2^4 \equiv 16 \equiv 1 \pmod{5}$, on a $(2^4)^2 \equiv 2^8 \equiv 1 \pmod{5}$, $2^{12} \equiv 2^8 2^4 \equiv 1 \pmod{5}$ et ainsi de suite. Donc, pour tout $k \geq 1$, $2^{4k} \equiv 1 \pmod{5}$.
3. On peut calculer $2^{32} \pmod{17}$, sans évaluer 2^{32}. En effet, on obtient de proche en proche $2^3 \equiv 8 \pmod{17}, 2^4 \equiv 16 \pmod{17}, 2^5 \equiv 32 \equiv 15 \pmod{17}, 2^{10} \equiv (2^5)^2 \equiv 15^2 \equiv 4 \pmod{17}, 2^{30} \equiv (2^{10})^3 \equiv 4^3 \equiv 64 \equiv 13 \pmod{17}, 2^{32} \equiv 2^{30}2^2 \equiv 13 \cdot 4 \equiv 52 \equiv 1 \pmod{17}$.

Proposition 2.6 *Si a, b, c, d et n sont des entiers, alors*

1. *Si* $a \equiv b \pmod{n}$ *et* $d|m$, *alors* $a \equiv b \pmod{d}$.
2. *Si* $ac \equiv bd \pmod{n}$, *alors* $a \equiv b \pmod{n/\mathrm{pgcd}\,(\mathrm{c}, \mathrm{n})}$.

Exemple 2.7
Montrons que $3|n^3 - n$, pour tout n. Comme ceci équivaut à montrer que $n^3 - n \equiv 0 \pmod{3}$, pour tout n et que tout nombre n est ou bien congru à $0, 1$ ou 2 modulo 3, il suffit de vérifier la relation ci-dessus pour ces trois valeurs. Or,

$$0^3 \equiv 0 \pmod{3},\ 1^3 - 1 \equiv 0 \pmod{3} \text{ et } 2^3 - 2 \equiv 0 \pmod{3}.$$

Par conséquent, $3|n^3 - n$, pour tout n.

Proposition 2.8 *Si* $\text{pgcd}\,(\text{m},\text{n}) = 1$, *alors* $\Big(a \equiv b \pmod{m}$ *et* $a \equiv b \pmod{n}\Big)$ *si et seulement si* $a \equiv b \pmod{mn}$.

Exemple 2.9

1. $a \equiv b \pmod{12}$ est équivalent à $\Big(a \equiv b \pmod{4}$ et $a \equiv b \pmod{3}\Big)$.

2. Si p et q sont des nombres premiers distincts et si a est un entier, alors $a^2 \equiv 1 \pmod{pq}$ si et seulement si $a^2 \equiv 1 \pmod{p}$ et $a^2 \equiv 1 \pmod{q}$.

Définition 2.10 *Soient a et n des nombres entiers. Un entier a' est appelé inverse de a modulo n si et seulement si* $aa' \equiv a'a \equiv 1 \pmod{n}$. *On dit que a est inversible modulo n, si a admet un inverse. Si a admet un inverse, alors cet inverse est unique modulo n.*

Exemple 2.11

1. Comme $2 \cdot 6 \equiv 1 \pmod{11}$, l'inverse de 6 modulo 11 est 2 et l'inverse de 2 modulo 11 est 6.

2. L'inverse de 3 modulo 8 est 3, car $3 \cdot 3 \equiv 1 \pmod{8}$.

3. 2 n'admet pas d'inverse modulo 8, parce que $2x \equiv 1 \pmod{8}$ implique que $8|2x-1$, ce qui est impossible, comme $2x - 1$ est toujours un nombre impaire.

Proposition 2.12 *Les éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *sont les entiers premiers avec n et forment un groupe pour la multiplication noté* $(\mathbb{Z}/n\mathbb{Z})^\star$.

preuve: Soit $a \in \mathbb{Z}/n\mathbb{Z}$. Alors, $au \equiv 1 \pmod{n}$ si et seulement s'il existe un entier v tel que $au - nv = 1$. Le théorème de Bezout implique que a et n sont alors premiers entre eux. □

Si p est un nombre premier, tous les entiers plus petits que p sont premiers avec p. Tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont donc inversibles et la propostion ci-dessus implique

Corollaire 2.13 *Si p est un nombre premier, alors* $\mathbb{Z}/p\mathbb{Z}$ *est un corps.*

Cela veut dire qu'on peut faire toutes les opérations de calcul habituelles avec les classes de congruences.

Comment calcule-t-on l'inverse x d'un entier u modulo n? Cet inverse est solution de l'équation

$$ux \equiv 1 \pmod{n}$$

Cela équivaut à dire qu'il existe un entier v tel que

$$ux - 1 = vn$$

c'est-à-dire

$$ux - vn = 1$$

Si u et v sont premiers entre eux, l'existence de x et y suit du théorème de Bezout et on les trouve en pratique en utilisant l'algorithme d'Euclide étendu.

3 Les théorèmes modulaires fondamentaux

Théorème 3.1 (des restes chinois) *Si $m_1, m_2, ..., m_k$ sont des entiers deux à deux premiers entre eux et si $a_1, a_2, ..., a_k$ sont des entiers quelconques, il existe un entier x tel que, pour tout $i = 1, ..., k$*

$$x \equiv a_i \pmod{m_i}.$$

Corollaire 3.2 *Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, alors*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Théorème 3.3 (Fermat) *Soit p un nombre premier. Alors, $a^p \equiv a \pmod{p}$, pour tout entier a. En particulier, si a et p sont premiers entre eux, $a^{p-1} \equiv 1 \pmod{p}$.*

Exemple 3.4

1. Montrons que $2^{50} + 3^{50}$ est divisible par 13.

   D'après le théorème de Fermat, $2^{12} \equiv 1 \pmod{13}$. Comme $50 = 4 \cdot 12 + 2$, on a $2^{50} \equiv 2^{4 \cdot 12+2} \equiv (2^{12})^4 2^2 \equiv 1 \cdot 4 \pmod{13}$. De plus, $3^{12} \equiv 1 \pmod{13}$, donc $3^{50} \equiv 3^{48}3^2 \equiv 9 \pmod{13}$. Par conséquent, $2^{50} + 3^{50} \equiv 4 + 9 \equiv 13 \equiv 0 \pmod{13}$.

2. Déterminons le reste de 3^{372} par 37.

   Comme 37 est un nombre premier, $3^{36} \equiv 1 \pmod{37}$. Or, $372 = 10 \cdot 36 + 12$, donc $3^{372} \equiv 3^{10 \cdot 36+12} \equiv (3^{36})^{10}3^{12} \equiv 1 \cdot 3^{12} \pmod{37}$. Comme $3^4 \equiv 81 \equiv 7 \pmod{37}, 3^{12} \equiv 7^3 \equiv 7 \cdot 49 \equiv 7 \cdot 12 \equiv 10 \pmod{37}$. Par conséquent, le reste cherché vaut 10.

Dans l'arithmétique des congruences, le nombre d'éléments inversibles joue un rôle important. Il apparaît entre autre dans la généralisation du théorème de Fermat aux nombres composés.

Définition 3.5 *On note $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. La fonction φ est appelée l'indicateur d'Euler.*

Exemple 3.6

1. $\varphi(8) = 4$, comme les éléments inversibles modulo 8 dans $\{0, 1, 2, ..., 7\}$ sont $1, 3, 5$ et 7.

2. $\varphi(p) = p - 1$, si p est un nombre premier, car $\mathrm{pgcd}\,(\mathrm{p}, \mathrm{a}) = 1$, pour tout a dans $\{1, 2, ..., p - 1\}$.

3. Si p est un nombre premier et r un entier positif, alors, il existe p^{r-1} multiples de p plus petits que p^r. Comme tous les autres nombres plus petits que p^r sont premiers avec p, on a

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

Proposition 3.7 *Si $\mathrm{pgcd}\,(\mathrm{m}, \mathrm{n}) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Corollaire 3.8 *Si* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, *alors*

$$\begin{aligned}\varphi(n) &= \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) \\ &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\end{aligned}$$

Exemple 3.9

$$\begin{aligned}\varphi(29 \cdot 5^2) &= \varphi(29)\varphi(5^2) \\ &= 28 \cdot 5^2 \left(1 - \tfrac{1}{5}\right) \\ &= 28 \cdot 20 \\ &= 560.\end{aligned}$$

Théorème 3.10 (Euler) *Si* a *et* n *sont des entiers premiers entre eux, alors* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

4 Le RSA

Le RSA est sans doute le cryptosystème à clef publique le plus utilisé. Sa sécurité est basée sur la difficulté de factoriser de très grands nombres entiers.

Expliquons son fonctionnement.

4.1 Génération des clés

L'entité B produit ses clés privé respectivement publique de la façon suivante: B détermine aléatoirement deux nombres premiers distincts p et q et calcule leur produit

$$n = p \cdot q.$$

De plus, B choisit un nombre entier e tel que

$$1 < e < \varphi(n) = (p-1)(q-1) \text{ et } \mathrm{pgcd}\left(\mathrm{e}, (\mathrm{p}-1)(\mathrm{q}-1)\right) = 1$$

et il calcule son inverse modulo $(p-1)(q-1)$, noté d. Comme $\mathrm{pgcd}\left(\mathrm{e}, (\mathrm{p}-1)(\mathrm{q}-1)\right) = 1$, cet inverse existe toujours. De plus, e est un nombre impair.

La clé publique est alors formé par la paire (n, e), la clé privée est d. On appelle n le module RSA, e l'exposant public et d l'exposant privé.

Exemple 4.1
B obtient les nombres premiers $p = 11$ et $q = 23$. Alors, $n = 253$ et $(p-1)(q-1) = 10 \cdot 22 = 2^2 \cdot 5 \cdot 11$. Le plus petit choix possible pour e est $e = 3$. Pour ce choix, on trouve $d = 147$.

Remarque 4.2
Dans la procédure de génération des clés pour le RSA, on peut remplacer la fonction $\varphi(n)$ par la fonction $\lambda(n) = (p-1)(q-1)/2$. Ceci a l'avantage d'obtenir un exposant privé plus petit, ce qui peut accélérer le déchiffrage.

4.2 Chiffrage

Supposons que le message à chiffrer soit représenté par le nombre entier m vérifiant $0 \leq m < n$. On le transforme dans le texte chiffré c en calculant

$$c \equiv m^e \pmod{n}.$$

Remarquons que ceci est bien possible, si on connaît la clé publique (n, e).

Exemple 4.3
Si $n = 253$ et $e = 3$, le nombre $m = 165$ est chiffé en $c \equiv 165^3 \pmod{253} = 110$.

4.3 Déchiffrage

Le déchiffrage du RSA se fait en utilisant le résultat suivant:

Théorème 4.4 *Soient (n, e), respectivement d, une clé RSA publique et la clé privée associée. Alors,*

$$(m^e)^d \equiv m \pmod{n}.$$

pour tout entier m tel que $0 \leq m < n$.

preuve:
Comme $ed \equiv 1 \pmod{(p-1)(q-1)}$, il existe un entier l tel que

$$ed = 1 + l(p-1)(q-1).$$

Ainsi,

$$(m^e)^d = m^{ed} = m^{1+l(p-1)(q-1)} = m(m^{(p-1)(q-1)l}).$$

Ceci implique que

$$(m^e)^d \equiv m(m^{p-1})^{(q-1)l} \equiv m \pmod{p}.$$

En effet, si p est un diviseur de m, cette congruence est triviale, puisque des deux côtés elle vaut 0. Sinon, le théorème de Fermat implique que $m^{p-1} \equiv 1 \pmod{p}$ et on obtient la congruence annoncé en élevant les deux côtés à la puissance $l(q-1)$ et en multipliant ensuite par m.

De même, on peut montrer que

$$(m^e)^d \equiv m \pmod{q}$$

Par conséquent, la proposition 2.8 implique que

$$(m^e)^d \equiv m \pmod{n}$$

□

Si un texte chiffré c a été obtenu d'un message original m, en utilisant le RSA, on peut donc le déchiffrer facilement en calculant

$$m = c^d \pmod{n},$$

sous condition de connaître la clé privée d.

Exemple 4.5
Revenons sur l'exemple de ce paragraphe. On avait $n = 253, e = 3$ et $d = 147$. De plus, on a chiffré le nombre $m = 165$ et obtenu le texte chiffré $c = 110$. Pour déchiffrer ce nombre, on calcule $110^{147} \pmod{253}$ dont le résultat est bel et bien $m = 165$.

Remarque 4.6
On peut réduire considérablement le temps de calcul pour le déchiffrage en utilisant le théorème des restes chinois.

En effet, au lieu de calculer $m = c^d \pmod{n}$, on peut calculer les deux quantités $m_p = c^d \pmod{p}$ et $m_q = c^d \pmod{q}$ et résoudre ensuite la double congruence

$$m \equiv m_p \pmod{p} \text{ et } m \equiv m_q \pmod{q}$$

Le théorème des restes chinois implique que cette congruence admet une solution. Pour la trouver, on utilise l'algorithme d'Euclide étendu pour déterminer des entiers y_p et y_q tels que

$$y_p p + y_q q = 1.$$

Alors,

$$m = (m_p y_q q + m_q y_p p) \pmod{n}.$$

Remarquons que les entiers $y_p p$ et $y_q q$ ne dépendent pas du message à déchiffrer et peuvent être calculés une fois pour toutes.

5 Factorisation

Théorème 5.1 (Euclide) *Il existe une infinité de nombres premiers.*

Théorème 5.2 *Tout nombre entier positif strictement supérieur à* 1 *peut être décomposé de façon unique comme produit de nombres premiers.*

Pour des entiers négatifs, on obtient la factorisation unique, en multipliant par -1 et en utilisant le théorème précédent.

Lemme 5.3 *Si a est un entier qui admet la factorisation en nombre premiers $a = p_1^{a_1} ... p_k^{a_k}$, alors un entier positif b divise a si et seulement si b admet une factorisation en nombres premiers de la forme $b = p_1^{b_1} ... p_k^{b_k}$, avec $0 \leq b_i \leq a_i$ pour $1 \leq i \leq k$.*

Comment trouve-t-on en pratique la décomposition en nombre premiers d'un entier n? La méthode la plus simple consiste à diviser n par tous les nombres premiers plus petits que $\sqrt{n}$, jusqu'à trouver un diviseur p. Puis, on applique la même méthode au nombre n/p et ainsi de suite. Cette méthode présuppose bien sûr que l'on dispose d'une table de tous les nombres premiers plus petits que $\sqrt{n}$. Elle devient vite inintéressante quand n devient grand.

La première méthode qui ne procède pas par divisions de test a été trouvé par Pierre de Fermat (1601-1665). Elle utilise le fait que si n peut être écrit comme différence de deux carrés alors sa factorisation est facile. En effet, alors

$$n = a^2 - b^2 = (a - b)(a + b).$$

Pour trouver une représentation d'un entier comme différence de deux carrés, on procède de la façon suivante: on cherche le premier carré a^2 supérieur à n, et on calcule $a^2 - n$. Si $a^2 - n = b^2$ pour un entier b, alors on a réussi, sinon on cherche le prochain carré supérieur à n et ainsi de suite.

6 Bibliographie

[1] Johannes Buchmann, *Einführung in die Kryptographie*, Springer-Verlag, 2001

[2] Ramanujachary Kumanduri & Cristina Romero, *Number Theory with Computer Applications*, Prentice Hall, 1998

[3] Robert Edward Lewand, *Cryptological Mathematics*, The Mathematical Association of America, 2000.