séminaire RSA

Bases mathématiques

Jang Schiltz
Enseignant - chercheur au Centre Universitaire de Luxembourg

contenu

- Divisibilité
- Arithmétique modulaire
- Les théorèmes fondamentaux
- Le RSA
- Le problème de la factorisation

chapitre 1

Cryptology & Security Initiative

Divisibilité

Résultats essentiels sur la divisibilité et les nombres premiers

- Arithmétique modulaire
- Thèorèmes fondamentaux
- Le RSA
- Le problème de la factorisation

définition de la divisibilité

Cryptology & Security Initiative

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* = a ·c.

On dit alors que *a* est un diviseur de *b* ou que *b* est divisible par *a.*

1er exemple de divisibilité

Cryptology & Security Initiative

$$24 = 2 \cdot 12 \quad \text{et} \quad 24 = 3 \cdot 8$$

- $2|24$ $12|24$ $3|24$ $8|24$

$$24 = (-2)(-12)$$

- $-2|24$ $-12|24$

2eme exemple de divisibilité

Cryptology & Security Initiative

Aucun entier non nul *a* n'est divisible par 0

Sinon, il existerait c tel que a = c·0

Mais, 0 = 0 ·c, pour tout c

⇓ 0|0

3eme exemple de divisibilité

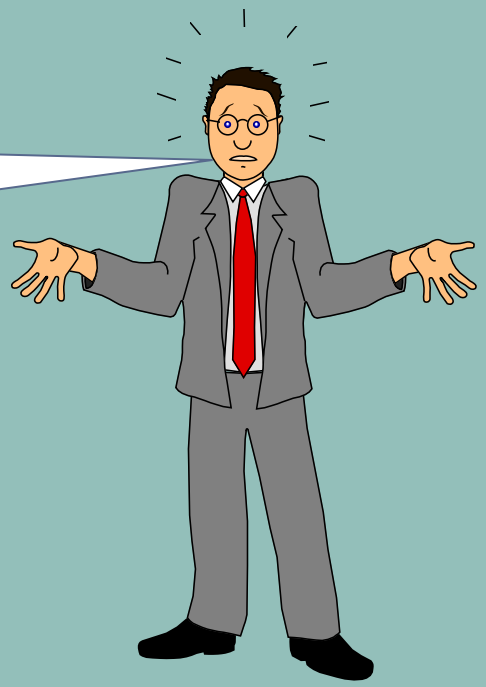
Cryptology & Security Initiative

Tout entier *a* divise 0.

En effet, 0 ·a = 0.

4^{eme} exemple de divisibilité

Quels sont les diviseurs entiers de 5?



Ce sont 1 et 5.

définition d'un nombre premier

Cryptology
& Security
Initiative

Un nombre entier positif $p > 1$ est appelé nombre premier si ses seuls diviseurs positifs sont 1 et p.

Un nombre non premier est dit nombre composé.

division euclidienne

Cryptology & Security Initiative

Soient deux entiers a et b, avec b ≠ 0.

Alors, il existe des entiers p et r uniques, tels que $a = bq + r$ et 0 ≤ r < |b|.

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

1er exemple de division euclidienne

$a = 37 \qquad b = 15$

$37 = 2 \cdot 15 + 7$

$\Downarrow \quad q = 2 \text{ et } r = 7$

2eme exemple de division euclidienne

$a = 37 \qquad b = -15$

$37 = (-2)(-15) + 7$

$\Rightarrow \quad q = -2 \text{ et } r = 7$

3eme exemple de division euclidienne

$a = -37 \qquad b = 15$

$-37 = -2 \cdot 15 - 7$

$q = -2$ et $r = -7$

Faux !, car r>0

3eme exemple de division euclidienne

$a = -37 \qquad b = 15$

$-37 = -3 \cdot 15 + 8$

$q = -3$ et $r = 8$

le pgcd

Cryptology & Security Initiative

On appelle plus grand commun diviseur des entiers *a* et de *b* et on note pgcd(*a*,*b*), le plus grand entier positif qui est à la fois diviseur de *a* et de *b*.

Exemple :

a = 12 b = 15

Diviseurs de 12: {1, 2, 3, 4, 6, 12}
Diviseurs de 15: {1, 3, 5, 15}

⇩ pgcd(12,15) = 3

entiers premiers entre eux

On dit que deux entiers *a* et *b* sont premiers entre eux si et seulement si pgcd(*a*,*b*) =1

Exemple : a = 7 b = 12

Diviseurs de 12: {1, 2, 3, 4, 6, 12}
Diviseurs de 7: {1, 7}

⇓ 7 et 12 sont premiers entre eux.

théorème de Bezout

Cryptology
& Security
Initiative

Deux entiers *a* et *b* sont premiers entre eux si et seulement s'il existe deux entiers *u* et *v* tels que

$$ua + vb = 1$$

chapitre 2

Cryptology & Security Initiative

Comment calculer modulo n?

Divisibilité

Arithmétique modulaire

Théorèmes fondamentaux

Le RSA

Le problème de la factorisation

définition de la congruence

Si *a*, *b* et *n* sont des entiers, on dit que *a* est congru à *b* modulo *n* et on note $a = b \pmod{n}$, si $n \mid a-b$

On dit aussi que *b* est un résidu de *a* modulo *n*, ou un reste de *a* modulo *n*.

1er exemple de congruence

Cryptology & Security Initiative

$$9 = 23 - 14$$

$$\Leftrightarrow \quad 23 = 14 \pmod 9$$

N'importe quels deux nombres de l'ensemble {…, -4, 5, 14, 23, …} sont congrus modulo 9.

2eme exemple de congruence

Pour tous entiers a et b, il existe c tel que
$b - a = c \cdot 1$

$\Leftrightarrow \quad a = b \pmod 1$

remarque sur les congruences

$a = b \pmod{n}$ si et seulement si
$a = b \pmod{-n}$.

Pour cette raison, on ne considère que des modules positifs.

relation d'équivalence

Cryptology
& Security
Initiative

Soient a, b, c et n des entiers.

$a = a \pmod n$

$a = b \pmod n$ ssi $b = a \pmod n$

Si $a = b \pmod n$ et $b = c \pmod n$,
alors $a = c \pmod n$

La congruence est une relation d'équivalence

remarque sur la relation d'équivalence

Cryptology
& Security
Initiative

Les classes d'équivalence de cette relation (classes de reste modulo n) sont

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

calcul avec les congruences

Cryptology & Security Initiative

Soient a, b, c, d et n des entiers.

Si $a = b \pmod n$, alors $ac = bc \pmod n$

Si $a = b \pmod n$ et $c = d \pmod n$,
alors $a + c = b + d \pmod n$

Si $a = b \pmod n$ et $c = d \pmod n$,
alors $ac = bd \pmod n$

Si $a = b \pmod n$, alors $a^k = b^k \pmod n$

1er exemple de calcul

Cryptology & Security Initiative

$$16 = -1 \pmod{17}$$

$$\Rightarrow 16^2 (=256) = 1 \pmod{17}$$

2^{eme} exemple de calcul

Cryptology & Security Initiative

$2^4 = 16 = 1 \pmod 5$

$\Rightarrow 2^8 = (2^4)^2 = 1 \pmod 5$

$\Rightarrow 2^{12} = 2^8\, 2^4 = 1 \pmod 5$

$\Rightarrow 2^{4k} = 1 \pmod 5$, pour tout k.

3eme exemple de calcul

$2^3 = 8 \pmod{17}$

$2^4 = 16 \pmod{17}$

$2^5 = 32 = 15 \pmod{17}$

$2^{10} = (2^5)^2 = 15^2 = 4 \pmod{17}$

$2^{30} = (2^{10})^3 = 4^3 = 64 = 13 \pmod{17}$

Comment calculer 2^{32} ?

$2^{32} = 2^{30}\,2^2 = 13 \cdot 4 = 52 = 1 \pmod{17}$

plus de calcul

Soient a, b, c, d et n des entiers.

Si $a = b \pmod n$ et $d|n$,
alors $a = b \pmod d$

Si $ac = bc \pmod n$,
alors $a = b \pmod{n/pgcd(c,n)}$

exemple

Cryptology & Security Initiative

Montrons que $3|n^3 - n$

Il faut montrer que
$n^3 - n = 0 \pmod 3$. Or,

$$\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$$

$0^3-0 = 0 \pmod 3$

$1^3-1= 0 \pmod 3$

$2^3-2= 0 \pmod 3$

$\Downarrow$ $3|n^3 - n$

équivalence

Si pgcd (m,n) = 1, alors

$[a = b \pmod m \text{ et } a = b \pmod n]$
$\Leftrightarrow a = b \pmod{mn}$

Si p et q sont des nombres premiers, alors
$a^2 = 1 \pmod{pq}$ ssi
$a^2 = 1 \pmod p$ et $a^2 = 1 \pmod q$

définition de l'inverse modulo n

Cryptology
& Security
Initiative

Soient a et n des entiers. Un entier a' est dit inverse de a modulo n si et seulement si aa' = a'a = 1 (mod n).

On dit que a est inversible modulo n, si a admet un inverse modulo n.

Si a admet un inverse modulo n, alors cet inverse est unique.

1er exemple d'inverse

Cryptology & Security Initiative

$$2 \cdot 6 = 1 \pmod{11}$$

- l'inverse de 2 modulo 11 est 6
- l'inverse de 6 modulo 11 est 2

2eme exemple d'inverse

$$3 \cdot 3 = 1 \pmod 8$$

- l'inverse de 3 modulo 8 est 3

3eme exemple d'inverse

$2x = 1 \pmod 8 \Leftrightarrow 8 | 2x-1$

Or, 2x-1 est impair et 8 est pair

$\Leftrightarrow$ 2 n'admet pas d'inverse modulo 8

éléments inversibles

Cryptology & Security Initiative

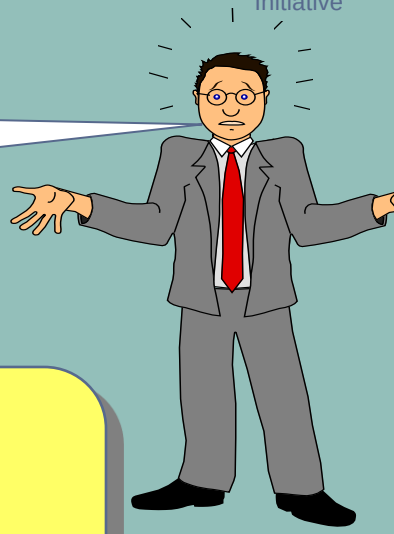
Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les entiers premiers avec n et forment un groupe pour la multiplication noté $(\mathbb{Z}/n\mathbb{Z})^*$.

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

calcul de l'inverse modulo n

Cryptology & Security Initiative

Comment calcule-t-on l'inverse x d'un entier u modulo n?



ux = 1 (mod n) ⇕ il existe v tel que ux - 1 = vn

Théorème de Bezout ⇕ existence de x et v, si u et n sont premiers entre eux.

Calcul pratique : algorithme d'Euclide étendu

chapitre 3

Cryptology & Security Initiative

Ce qu'il faut savoir pour comprendre les détails

Divisibilité

Arithmétique modulaire

Théorèmes fondamentaux

Le RSA

Le problème de la factorisation

le théorème chinois

Cryptology & Security Initiative

Si $m_1, m_2, ..., m_k$ sont des entiers deux à deux disjoints entre eux et si $a_1, a_2, ..., a_k$ sont des entiers quelconques, il existe un entier x tel que, pour tout $i = 1, ..., k$

$$x = a_i \pmod{m_i}$$

corollaire

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

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

théorème de Fermat

Si p est un nombre premier, alors

$a^p = a \pmod p$, pour tout a.

Si pgcd(a,p)=1,

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

exemple 1

Cryptology & Security Initiative

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

Fermat ⇓ $2^{12} = 1 \pmod{13}$

$50 = 4 \cdot 12 + 2$

⇓ $2^{50} = (2^{12})^4 \, 2^2 = 1 \cdot 4 = 4 \pmod{13}$

Fermat ⇓ $3^{12} = 1 \pmod{13}$

⇓ $3^{50} = (3^{12})^4 \, 3^2 = 1 \cdot 9 = 9 \pmod{13}$

⇓ $2^{50} + 3^{50} = 4 + 9 = 13 = 0 \pmod{13}$

exemple 2

Cryptology & Security Initiative

Cherchons le reste de 3^{372} par 37

Fermat ⇓ $3^{36} = 1 \pmod{37}$

$372 = 10 \cdot 36 + 12$

$3^4 = 81 = 7 \pmod{37}$ ⇓ $3^{12} = 7^3 = 7 \cdot 49 = 7 \cdot 12 = 10 \pmod{37}$

⇓ $3^{372} = (3^{36})^{10} 3^{12} = 1 \cdot 10 = 10 \pmod{37}$

⇓ $3^{372} = 10 \pmod{37}$

l'indicateur d'Euler

Cryptology & Security Initiative

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 : n = 8

Les éléments inversibles modulo 8 dans {0,1,2,…,7} sont {1, 3, 5, 7}

⇓ $\varphi(8) = 4$

autres exemples

p premier ⇓ pgcd(p,a) = 1, ∀a ∈ {1,…,p-1}

⇓ $\varphi(p) = p-1$

p premier, r entier

⇓ $\varphi(p^r) = p^r - p^{r-1} = p^r (1-1/p)$

propriétés de l'indicateur d'Euler

Cryptology & Security Initiative

Si pgcd(m,n) = 1,
alors $\varphi(mn) = \varphi(m)\varphi(n)$.

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

$$\varphi(n) = \prod_{k=1}^{n} p_i^{\alpha_{i-1}} (p_i - 1)$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

exemple d'application

$$\varphi(29 \cdot 5^2) = \varphi(29)\varphi(5^2)$$
$$= 28 \cdot 5^2(1\text{-}1/5)$$
$$= 28 \cdot 20$$
$$= 560$$

Théorème d'Euler

Si a et n sont des entiers premiers entre eux, alors $a^{\varphi(n)} = 1 (\mathrm{mod}\, n)$.

chapitre 4

Cryptology & Security Initiative

Description élémentaire du cryptosystème

Divisibilité

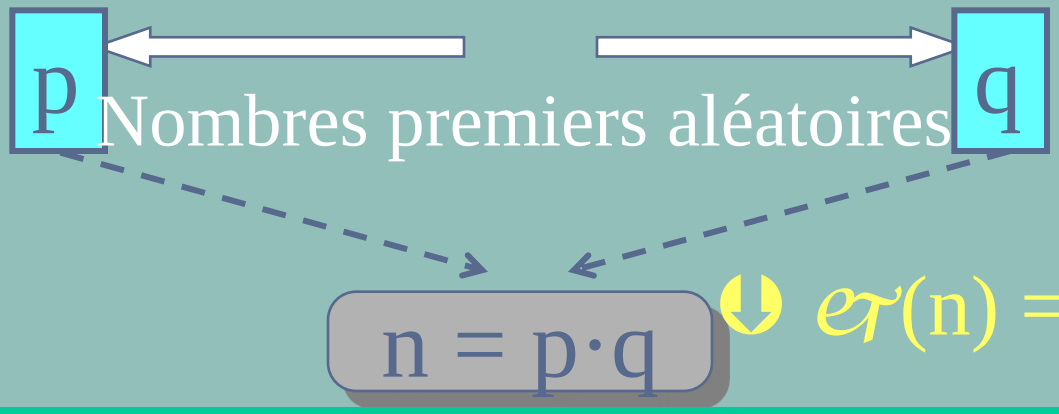
Arithmétique modulaire

Théorèmes fondamentaux

Le RSA

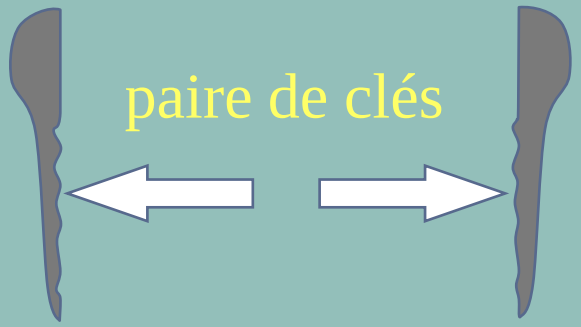
Le problème de la factorisation

génération des clés



On choisit e tel que
$1 < e < \varphi(n)$ et $pgcd(e,\varphi(n)) = 1$

On calcule d tel que $ed = 1 \pmod{\varphi(n)}$



Clé publique (n,e)

Clé privée d

exemple de clés

Cryptology & Security Initiative

$p = 11$ et $q = 23$

$\Rightarrow n = 253$ et $(p-1)(q-1) = 10 \cdot 22 = 2^2 \cdot 5 \cdot 11$

Le plus petit choix pour e est $e = 3$

$\Rightarrow d = 147$

Remarque : Parfois, on remplace la fonction $\varphi(n)$ par $\lambda(n) = (p-1)(q-1)/2$
$\Rightarrow$ accélération du déchiffrage

procédure de chiffrage

Message m
$0 \leq m < n$

Texte chiffré
$c = m^e \pmod{n}$

Exemple:

$n = 253$ et $e = 3$

$m = 165 \Rightarrow c = 165^3 \pmod{253}$

$\Rightarrow c = 110$

procédure de déchiffrage

Texte chiffré c → Message original $m = c^d \pmod n$

Exemple:

$n = 253, e = 3, d = 147$

$c = 110 \Rightarrow m = 110^{147} \pmod{253}$

$\Rightarrow m = 165$

preuve de la procédure de déchiffrage

$ed = 1 \pmod{(p-1)(q-1)}$

$\Rightarrow \exists k$ tel que $ed = 1+k(p-1)(q-1)$

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

1. Si $p|m$, $(m^e)^d = 0 \pmod{p}$ et $m(m^{k(p-1)(q-1)}) = 0 \pmod{p}$
2. Sinon Fermat $\Rightarrow m^{p-1} = 1 \pmod{p}$

et $(m^e)^d = m(m^{(p-1)})^{k(q-1)} = m \pmod{p}$

Finalement $(m^e)^d = c^d = m \pmod{p}$

De même, $c^d = m \pmod{q}$

Théorème d'équivalence $\Rightarrow c^d = m \pmod{n}$

□

remarque sur le déchiffrage

On peut réduire considérablement le temps de calcul du déchiffrage en utilisant le thèorème chinois.

~~$m = c^d \pmod n$~~

$$m_p = c^d \pmod p$$

$$m_q = c^d \pmod q$$

Théorème des restes chinois

$$m = m_p \pmod p$$

$$m = m_q \pmod q$$

chapitre 5

Cryptology & Security Initiative

Quelques idées de base

- Divisibilité
- Arithmétique modulaire
- Théorèmes fondamentaux
- Le RSA

Le problème de la factorisation

théorèmes

Cryptology
& Security
Initiative

Théorème d'Euclide :
Il existe une infinité de nombres premiers.

Théorème arithmétique fondamental:
Tout nombre entier peut être décomposé de façon unique comme produit de nombres premiers.

méthodes de factorisation

Méthode exhaustive :

On divise n par tous les entiers entre 1 et $\sqrt{n}$ jusqu'à trouver un diviseur d. Puis, on recommence avec n/d.

Méthode de Pierre de Fermat (1601-1665) :

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

En pratique, on calcule $a^2 - n$, ou a^2 est le plus petit carré > n.

Si c'est un carré, on a trouvé.

Sinon, on essaie le carré prochain.