Outils arithmétiques pour la méthode RSA

Malika More
(malika.more@iut.u-clermont1.fr)
Jean Mailfert - Gisèle Provost

1A - IUT Info - Clermont 1

Arithmétique et Cryptographie

Année 2011-2012

Important

- Les transparents du cours et d'autres documents et informations sont disponibles sur la page du cours sur l'ENT
- Il est très fortement recommandé d'apporter une calculatrice en cours et en TD d'arithmétique

Plan du cours

Il y a un problème

La situation suivante se présente souvent quand on traite à la main des exercices sur la méthode RSA et fait l'objet de ce paragraphe.

Problème

On veut calculer $5^{13} \mod 187$. La calculatrice refuse.

Remarque

En fait, ça dépend des calculatrices !
Mais le problème est le même pour calculer $40^{384} \mod 187$
Et là, toutes les calculatrices refusent...

La cause du problème

- La raison de ce refus est que le résultat intermédiaire 5^{13} est trop grand pour être calculé exactement avec une calculatrice.
- On obtient seulement une valeur approchée en notation scientifique.
- Cependant, on sait à l'avance que le résultat final sera forcément inférieur à 187, puisqu'on calcule modulo 187.
- La méthode expliquée ci-dessous permet de ne pas passer par des résultats intermédiaires qui dépassent les capacités des calculatrices.
- En effet, tous les nombres qu'on sera amené à manipuler seront inférieurs à $187^2 = 34969$.

Rappels sur les exposants

Avant d'en venir à la solution du problème, on rappelle quelques propriétés utiles sur les exposants :

Propriétés

Quels que soient les entiers naturels a, b, c, on a :

1. $a^{(2^0)} = a$
2. $a^{(2^{b+1})} = (a^{(2^b)})^2$
3. *Attention :* $a^{(b^c)} \neq (a^b)^c$. *Par exemple* $5^{(2^3)} = 5^8$ *mais* $(5^2)^3 = 5^{2\times 3} = 5^6$.
4. $a^{(2^b+2^c)} = a^{(2^b)} \times a^{(2^c)}$

Application

Exemple

Quand on prend comme exposant les puissances de 2 successives, on obtient une suite d'élévations au carré :

$5^{(2^0)} = 5$
$5^{(2^1)} = 5^{(2^{0+1})} = (5^{(2^0)})^2 = 5^2 = 25$
$5^{(2^2)} = 5^{(2^{1+1})} = (5^{(2^1)})^2 = 25^2 = 625$
$5^{(2^3)} = 5^{(2^{2+1})} = (5^{(2^2)})^2 = 625^2 = 390625$
etc.

Exponentiation modulaire rapide

Solution

- On écrit l'exposant 13 en binaire, c.-à-d.

$$13_{dec} = 1101_{bin}$$

Autrement dit, on a $13 = 2^3 + 2^2 + 2^0$, donc :

$$5^{13} = 5^{(2^3+2^2+2^0)} = 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)}$$

- En passant au modulo, on a toujours :

$$5^{13} \equiv 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)} \mod 187$$

Il nous suffit donc de connaître $5^{(2^0)} \mod 187$, $5^{(2^2)} \mod 187$ et $5^{(2^3)} \mod 187$.

Exponentiation modulaire rapide

Solution (suite)

- On calcule les restes modulo 187 des carrés successifs de 5 jusqu'à la plus grande valeur dont on a besoin :

$$\begin{array}{lcll} 2^0 & \rightsquigarrow & 5^{(2^0)} \mod 187 & \rightsquigarrow \quad 5 \equiv 5 \mod 187 \\ 2^1 & & 5^{(2^1)} \mod 187 & \quad 5^2 \equiv 25 \mod 187 \\ 2^2 & & 5^{(2^2)} \mod 187 & \quad 25^2 \equiv 625 \equiv 64 \mod 187 \\ 2^3 & & 5^{(2^3)} \mod 187 & \quad 64^2 \equiv 4096 \equiv 169 \mod 187 \end{array}$$

- On prend les restes correspondant aux puissances qui nous intéressent (2^3, 2^2 et 2^0) :

$$5^{13} \equiv 5^{(2^3)} \times 5^{(2^2)} \times 5^{(2^0)} \equiv 169 \times 64 \times 5 \equiv 54080 \equiv 37 \mod 187$$

Ça marche à chaque fois

Exemple

- On veut calculer $174^{37} \mod 187$.
- On écrit l'exposant 37 en binaire, c.-à-d.

$$37_{dec} = 100101_{bin}$$

Autrement dit, on a $37 = 2^5 + 2^2 + 2^0$, donc :

$$174^{37} = 174^{(2^5)} \times 174^{(2^2)} \times 174^{(2^0)}$$

Ça marche à chaque fois

Exemple (suite)

- On calcule les restes modulo 187 des carrés successifs de 174 jusqu'à la plus grande valeur dont on a besoin :

$$\begin{array}{lll} 2^0 & \rightsquigarrow & 174 \equiv 174 \mod 187 \\ 2^1 & & 174^2 \equiv 30276 \equiv 169 \mod 187 \\ 2^2 & & 169^2 \equiv 28561 \equiv 137 \mod 187 \\ 2^3 & & 137^2 \equiv 18769 \equiv 69 \mod 187 \\ 2^4 & & 69^2 \equiv 4761 \equiv 86 \mod 187 \\ 2^5 & & 86^2 \equiv 7396 \equiv 103 \mod 187 \end{array}$$

- On prend les restes correspondant aux puissances qui nous intéressent (2^5, 2^2 et 2^0) :

$$174^{37} \equiv 174^{(2^5)} \times 174^{(2^2)} \times 174^{(2^0)} \equiv 103 \times 137 \times 174 \equiv 2455314 \equiv 4 \mod 187$$

À vous de jouer !

1. En utilisant la méthode d'exponentiation modulaire rapide, calculer $16^{23} \mod 19$.
2. Calculer le nombre de multiplications et d'élévations au carré que vous avez utilisées.

Exercice 1

En utilisant la méthode d'exponentiation modulaire rapide, calculer :

1. $51^{21} \mod 8$;
2. $231^{545} \mod 173$;
3. $51447^{6478} \mod 3241$.

Exercice 2

Calculer le nombre de multiplications et d'élévations au carré que vous devez faire en utilisant la méthode d'exponentiation rapide pour élever un nombre à la puissance 10262.

Un théorème crucial pour RSA

Théorème (Fermat)

Soit p un nombre premier et soit a un entier premier avec p. Alors on a

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

Exemple

- Prenons $p = 3$, qui est premier
- Et $a = 25$, qui est premier avec 3.
- On calcule $a^{(p-1)} = 25^{(3-1)} = 25^2 = 625$.
- Or on a $625 = 1 + 3 \times 208$, autrement dit on a bien

$$25^{(3-1)} \equiv 1 \mod 3$$

D'où ça vient ?

Une autre façon de le dire

- Dire que $a^{(p-1)} \equiv 1 \mod p$ équivaut à dire que

$$a^{(p-1)} - 1 \equiv 0 \mod p$$

- Ou encore que p divise $a^{(p-1)} - 1$

Comment faire ?

Stratégie

- On va plutôt voir que p divise $(a^{(p-1)} - 1) \times (p-1)!$
- C'est en fait équivalent : comme p est premier, p ne peut pas diviser $(p-1)!$ et doit forcément diviser l'autre facteur, c'est-à-dire $a^{(p-1)} - 1$

Réécritures

On repasse au modulo

- On remarque que

$$(a^{(p-1)} - 1) \times (p-1)! = a^{(p-1)} \times (p-1)! - (p-1)!$$

- Dire que p divise $(a^{(p-1)} - 1) \times (p-1)!$ revient à dire que $a^{(p-1)} \times (p-1)! - (p-1)! \equiv 0 \mod p$
- Ou encore que

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

Notation

On introduit une notation

- On remarque que $a^{(p-1)} \times (p-1)! = a \times 2a \times 3a \times \ldots \times (p-1)a$
- C'est pourquoi on introduit les notations $n_1 = a$, $n_2 = 2a$, $n_3 = 3a$, ..., $n_{p-1} = (p-1)a$
- Et on a $a^{(p-1)} \times (p-1)! = n_1 \times n_2 \times n_3 \times \ldots \times n_{p-1}$

Utilisation des restes

Conséquences

- Comme on travaille « modulo p », on note aussi $r_1 \equiv n_1 \mod p, \ldots, r_{p-1} \equiv n_{p-1} \mod p$
- Autrement dit, les r_k sont les restes modulo p des n_k.
- Pour tout $k = 1, \ldots, p-1$, on a $0 \leq r_k \leq p-1$
- Et bien sûr $n_1 \times \ldots \times n_{p-1} \equiv r_1 \times \ldots \times r_{p-1} \mod p$
- Il reste à vérifier que $r_1 \times \ldots \times r_{p-1} = (p-1)!$

Un dernier effort !

Pour montrer que $r_1 \times \ldots \times r_{p-1} = (p-1)!$

- On va vérifier que les nombres r_k sont tous non nuls et deux à deux distincts
- Et comme il y en a $p-1$ et qu'ils sont tous dans l'ensembles $\{0, \ldots, p-1\}$
- On aura démontré ce qu'on voulait

Allons-y...

Première étape : $r_k \neq 0$

- Chaque n_k n'est pas divisible par p
- En effet, $n_k = k \times a$ avec $1 \leq k \leq p-1$ et a premier avec p
- Et comme p est premier, c'est bien vrai
- On a donc $n_k \not\equiv 0 \mod p$, i.e. $r_k \neq 0$

Et pour finir...

Deuxième (et dernière) étape : $r_k \neq r_{k'}$

- Soit $1 \leq k < k' \leq p-1$
- On a aussi $1 \leq k' - k \leq p-1$
- Donc p ne divise pas $k' - k$
- Et donc p ne divise pas non plus $n_{k'} - n_k = k'a - ka = (k' - k)a$
- Ce qui veut dire que $r_{k'} - r_k \neq 0$

Ouf, c'est fini :-)

À vous de jouer !

1. Sans utiliser de calculatrice, montrer que 11 divise $15^{10} - 1$.
2. Sans utiliser de calculatrice, montrer que 13 divise $15^{12} - 1$.
3. En déduire que $15^{60} \equiv 1 \mod 143$.

À vous de jouer !

1. Montrer que lorsque p est premier, quel que soit le nombre a, on a $a^p \equiv a \mod p$.
2. Quels sont les nombres premiers p tels que p divise $2^p + 1$?

Exercice 3

Prouver que pour tout entier $n \geq 1$, 7 divise $3^{6n} - 1$.

Exercice 4

Montrer que les nombres 4^{20}, 9^{20}, 16^{20}, 25^{20}, 36^{20} et 49^{20} ont tous comme reste 1 dans la division par 41.

Exercice 5

Montrer, sans utiliser de calculatrice, que $17^{22} - 1$ est divisible par 23. En déduire le reste de 17^{156} modulo 23.

Exercice 6

1. Déterminer un entier p tel que $10^p - 1$ soit divisible par 401. On admettra que 401 est premier.
2. Montrer que $10^p - 1$ est aussi divisible par 9.
3. Montrer qu'il existe un multiple de 401 qui s'écrit avec le seul chiffre 1, c.-à-d. 1111...1111.
4. En déduire qu'il existe un multiple de 2005 qui s'écrit avec le seul chiffre 5, c.-à-d. 5555...5555.

Exercice 7

En utilisant la méthode d'exponentiation modulaire rapide, calculer :

1. $84^{18} \mod 9$;
2. $156^{312} \mod 38$;

Exercice 8

Calculer le nombre de multiplications et d'élévations au carré que vous devez faire en utilisant la méthode d'exponentiation rapide pour élever un nombre à la puissance 7645.

Exercice 9

Prouver que pour tout entier $n \geq 1$, on a $10^{16n} \equiv 1 \mod 17$.

Exercice 10

1. Pour fabriquer son code "sac-à-dos", Alice choisit le sac-à-dos facile $SADF = [3, 7, 14, 30, 57]$. Vérifiez qu'il s'agit bien d'un sac-à-dos facile.
2. Puis elle choisit le module $M = 123$. Pourquoi est-il acceptable ?
3. Ensuite, elle choisit le compliqueur $E = 22$. Pourquoi est-il acceptable ?
4. Calculez le sac-à-dos difficile $SADD$ d'Alice.
5. Calculez le faciliteur D correspondant au compliqueur E.
6. Alice va maintenant publier la partie publique de son code. Indiquez de quoi est constituée cette partie publique.
7. Alice reçoit le message crypté $mess = 121$. Déchiffrez ce message, c'est-à-dire déterminez le mot de 5 bits correspondant. Le bit de poids fort du message correspond au premier élément du sac-à-dos.
8. Bob souhaite envoyer à Alice le message binaire 1101011011. Chiffrez ce message. Pour chaque bloc, le bit de poids fort du message correspond au premier élément du sac-à-dos.

Exercice 11

Le code secret "sac-à-dos" d'Alice est constitué du sac-à-dos facile $SADF_A = [f_1^A, f_2^A, f_3^A, f_4^A, f_5^A]$, du sac-à-dos difficile $SADD_A = [d_1^A, d_2^A, d_3^A, d_4^A, d_5^A]$, du module M_A et du faciliteur c_A.

Le code secret "sac-à-dos" de Bob est constitué du sac-à-dos facile $SADF_B = [f_1^B, f_2^B, f_3^B, f_4^B]$, du sac-à-dos difficile $SADD_B = [d_1^B, d_2^B, d_3^B, d_4^B]$, du module M_B et du faciliteur c_B.

Alice veut envoyer à Bob le message binaire $mess = 011011011100011000101$.

Quels calculs Alice doit-elle effectuer pour chiffrer son message $mess$? Pour chaque bloc, le bit de poids fort du message correspond au premier élément du sac-à-dos.

FIN