UE MA9W05

Algorithmique de la cryptographie à clés publiques

Master mentions *Mathématiques* et *Informatique*

Enseignant responsable : Jean-Marc Couveignes.

Examen du 20/12/2013, de 8h30 à 11h30 (trois heures)

⋆⋆⋆

Calculette autorisée. Documents non-autorisés.

⋆⋆⋆

Ce sujet comporte cinq pages.

La notation accordera la plus grande importance à la qualité de la rédaction.

Exercice 1 : Énoncez le petit théorème de Fermat.

Quel est le pgcd de

$$2^{12012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012012}-1$$

et 143. Vous justifierez votre réponse.

Exercice 2 :

Factorisez 143.

Décrivez l'ensemble $\mathcal{S}$ des entiers x qui vérifient la congruence $x^{103} = 2 \bmod 143$.

Soit a un entier. Soit $\mathcal{T}_a$ l'ensemble des entiers x qui vérifient $x^{57} = a \bmod 143$.

Décrivez $\mathcal{T}_2$.

Décrivez $\mathcal{T}_8$.

Décrivez $\mathcal{T}_a$ pour un entier a quelconque. Vous distinguerez plusieurs cas.

Exercice 3 :

On pose $p = 331$. Montrez que p est un nombre premier.

Factorisez $p - 1$ en produit de facteurs premiers.

On vérifie que $2^{165} = 330 \bmod p$, $2^{110} = 299 \bmod p$, $2^{66} = 64 \bmod p$, $2^{30} = 1 \bmod p$, $5^{165} = 1 \bmod p$, $5^{110} = 31 \bmod p$, $5^{66} = 64 \bmod p$, $5^{30} = 180 \bmod p$.

Donnez un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

On pose $b = 329 \bmod p$ et on admet que $b^{165} = 1 \bmod p$, $b^{110} = 299 \bmod p$, $b^{66} = 64 \bmod p$, $b^{30} = 1 \bmod p$.

En utilisant la méthode de Pohlig-Hellman et le théorème des restes chinois, calculez un entier ℓ tel que b soit égal à $5^{\ell} \bmod p$. Vous détaillerez et justifierez les calculs.

Exercice 4 :

Soit $f(x)$ le polynôme $x^5 + x^4 + 1$ dans $\mathbb{F}_2[x]$.

Factorisez $f(x)$.

On pose $\mathbf{K} = \mathbb{F}_2[x]/f(x)$.

$\mathbf{K}$ est-il un corps ? Pourquoi ?

Résoudre l'équation $a^{11} = x \bmod f(x)$ où l'inconnue a appartient à $\mathbf{K}$.

Résoudre l'équation $x^\ell = 1 + x^2 \bmod f(x)$ où l'inconnue ℓ est un entier.

Exercice 5 :

Soit

$$n=2\times3^{72}\times5^{94}+1=22747870282497724867764266166467529168034703562947520329206099742869184865412535145878791809082031251.$$

On veut calculer $2^{(n-1)/2} \bmod p$. Comment faire ?

On trouve

$$2^{(n-1)/2}=22747870282497724867764266166467529168034703562947520329206099742869184865412535145878791809082031250 \bmod n.$$

On calcule aussi

$$2^{(n-1)/3}=11791219678163940506615639138405431889788864963308512559814102611481363493589902969729020027163691504 \bmod n,$$

$$2^{(n-1)/5}=21654376330887561819730743112521290573534764125875638216950517656429881743275862730524129927387779523 \bmod n.$$

Peut-on dire si n est premier ou composé. Justifiez précisément votre réponse.

Soit maintenant

$$m=2\times3^{72}\times5^{93}+1=45495740564995449735528532332935058336069407125895040658412199485738369730825070291757583618164062 51.$$

On trouve

$$2^{(m-1)/2}=32815304723083971513670769515038344994439803412126876651404613912714866061773743293914676597580344 15 \bmod m,$$

$$2^{(m-1)/3}=43822806908523801755571170461345730471796315201579913766723653442679645975418501931056952936009786 51 \bmod m,$$

$$2^{(m-1)/5}=45412193204219096024517806440291228370677880322404119304483990264740634351953770762029955337996480 80 \bmod m.$$

Peut-on dire si m est premier ou composé. Justifiez précisément votre réponse.

Exercice 6 :

Expliquez comment calculer une racine carrée modulo un nombre premier congru à 3 modulo 4. Vous illustrerez votre explication par un exemple.

Décrivez une application cryptographique de ces nombres premiers congrus à 3 modulo 4. Vous l'illustrerez sur un exemple.

On veut montrer (par l'absurde) qu'il existe une infinité de tels nombres premiers. On suppose donc qu'il existe un nombre fini de nombres premiers congrus à 3 modulo 4. On les nomme p_i pour i de 1 à I. On pose $P = 4 \times \prod_{1 \leq i \leq I} p_i - 1$

Montrez que l'un au moins des diviseurs premiers de P est congru à 3 modulo 4. On l'appelle q.

Montrez que q n'est pas l'un des p_i. Conclure.

Exercice 7 :

Donnez, s'il en existe, un entier n qui soit congru à 5 modulo 6, à 11 modulo 15, à 1 modulo 10.

Donnez, s'il en existe, un entier n qui soit congru à 1 modulo 2, à -1 modulo 3, à 3 modulo 5, à 4 modulo 7.

Exercice 8 :

Combien de chiffres comporte la représentation décimale de 34^{12}.

Donnez une formule générale (que vous justifierez) pour le nombre de chiffres dans la représentation décimale d'un entier positif n.

Combien de bits comporte la représentation binaire de 34^{12}.

Donnez une formule générale (que vous justifierez) pour le nombre de bits dans la représentation binaire d'un entier positif n.

Exercice 9 :

On veut factoriser le nombre $N = 32399$ en utilisant le crible quadratique.

1 . On note que $\sqrt{N} \simeq 179.9$. Écrivez une congruence modulo N du type

$$(a+m)^2 \equiv a^2 + u_1 a + u_0 \bmod N$$

dépendant d'un paramètre entier a. Ici m, u_0, u_1 sont des constantes entières bien choisies.

2 . Cherchez des valeurs de a comprises entre -40 et 40 qui permettent d'obtenir une congruence entre un carré et un nombre friable (dans un sens que vous préciserez) modulo N. On pourra utiliser le document ci-après.

```
for(a=-40,40,print([a,factor(a^2+2*a*180+1)]))
[-40, [-1, 1; 12799, 1]]
[-39, [-1, 1; 2, 1; 11, 1; 569, 1]]
[-38, [-1, 1; 5, 1; 2447, 1]]
[-37, [-1, 1; 2, 1; 5, 2; 239, 1]]
[-36, [-1, 1; 107, 1; 109, 1]]
[-35, [-1, 1; 2, 1; 11, 2; 47, 1]]
[-34, [-1, 1; 11083, 1]]
[-33, [-1, 1; 2, 1; 5, 1; 13, 1; 83, 1]]
[-32, [-1, 1; 5, 1; 2099, 1]]
[-31, [-1, 1; 2, 1; 5099, 1]]
[-30, [-1, 1; 19, 1; 521, 1]]
[-29, [-1, 1; 2, 1; 4799, 1]]
[-28, [-1, 1; 5, 1; 11, 1; 13, 2]]
[-27, [-1, 1; 2, 1; 5, 1; 29, 1; 31, 1]]
[-26, [-1, 1; 19, 1; 457, 1]]
[-25, [-1, 1; 2, 1; 53, 1; 79, 1]]
[-24, [-1, 1; 11, 1; 733, 1]]
[-23, [-1, 1; 2, 1; 5, 3; 31, 1]]
[-22, [-1, 1; 5, 1; 1487, 1]]
[-21, [-1, 1; 2, 1; 3559, 1]]
[-20, [-1, 1; 13, 1; 523, 1]]
```

```
[-19, [-1, 1; 2, 1; 41, 1; 79, 1]]
[-18, [-1, 1; 5, 1; 1231, 1]]
[-17, [-1, 1; 2, 1; 5, 1; 11, 1; 53, 1]]
[-16, [-1, 1; 5503, 1]]
[-15, [-1, 1; 2, 1; 13, 1; 199, 1]]
[-14, [-1, 1; 29, 1; 167, 1]]
[-13, [-1, 1; 2, 1; 5, 1; 11, 1; 41, 1]]
[-12, [-1, 1; 5, 2; 167, 1]]
[-11, [-1, 1; 2, 1; 19, 1; 101, 1]]
[-10, [-1, 1; 3499, 1]]
[-9, [-1, 1; 2, 1; 1579, 1]]
[-8, [-1, 1; 5, 1; 563, 1]]
[-7, [-1, 1; 2, 1; 5, 1; 13, 1; 19, 1]]
[-6, [-1, 1; 11, 1; 193, 1]]
[-5, [-1, 1; 2, 1; 887, 1]]
[-4, [-1, 1; 1423, 1]]
[-3, [-1, 1; 2, 1; 5, 1; 107, 1]]
[-2, [-1, 1; 5, 1; 11, 1; 13, 1]]
[-1, [-1, 1; 2, 1; 179, 1]]
[0, matrix(0,2)]
[1, [2, 1; 181, 1]]
[2, [5, 2; 29, 1]]
[3, [2, 1; 5, 1; 109, 1]]
[4, [31, 1; 47, 1]]
[5, [2, 1; 11, 1; 83, 1]]
[6, Mat([13, 3])]
[7, [2, 1; 5, 1; 257, 1]]
[8, [5, 1; 19, 1; 31, 1]]
[9, [2, 1; 11, 1; 151, 1]]
[10, Mat([3701, 1])]
[11, [2, 1; 13, 1; 157, 1]]
[12, [5, 1; 19, 1; 47, 1]]
[13, [2, 1; 5, 2; 97, 1]]
[14, Mat([5237, 1])]
[15, [2, 1; 29, 1; 97, 1]]
[16, [11, 1; 547, 1]]
[17, [2, 1; 5, 1; 641, 1]]
[18, [5, 1; 1361, 1]]
[19, [2, 1; 13, 1; 277, 1]]
[20, [11, 1; 691, 1]]
[21, [2, 1; 4001, 1]]
[22, [5, 1; 41, 2]]
[23, [2, 1; 5, 1; 881, 1]]
[24, [13, 1; 709, 1]]
[25, [2, 1; 4813, 1]]
[26, Mat([10037, 1])]
[27, [2, 1; 5, 2; 11, 1; 19, 1]]
```

```
[28, [5, 1; 41, 1; 53, 1]]
[29, [2, 1; 5641, 1]]
[30, Mat([11701, 1])]
[31, [2, 1; 11, 1; 19, 1; 29, 1]]
[32, [5, 1; 13, 1; 193, 1]]
[33, [2, 1; 5, 1; 1297, 1]]
[34, Mat([13397, 1])]
[35, [2, 1; 31, 1; 223, 1]]
[36, [53, 1; 269, 1]]
[37, [2, 1; 5, 1; 13, 1; 113, 1]]
[38, [5, 3; 11, 2]]
[39, [2, 1; 31, 1; 251, 1]]
[40, Mat([16001, 1])]
```

3 . Écrivez proprement toutes les congruences intéressantes obtenues. Portez les signes et les valuations dans une matrice M à coefficients entiers.

4 . Calculez le noyau de la réduction modulo 2 de la matrice M. Donnez la dimension de ce noyau, ainsi qu'une base.

5 . Pour chaque élément de cette base écrivez une congruence entre deux carrés modulo N. En déduire une factorisation (éventuellement triviale) de N.

Exercice 10 :

Rappelez la définition du symbole de Legendre.

Rappelez la définition du symbole de Jacobi.

Énoncez la loi de réciprocité quadratique.

En utilisant cette loi, calculez le symbole de Jacobi $\left(\frac{4673}{5352499}\right)$.

Vous détaillerez et justifierez les calculs.

Exercice 11 :

Soit $p = 6761$. On admet que p est premier. Soit $g = 765 \bmod p$.

Quelles congruences doit on vérifier pour s'assurer que g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

On admet que g est en effet un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ et on pose $h = 456 \bmod p$.

On veut calculer le logarithme discret de h en base g.

Décrivez un algorithme rapide pour ce faire.

On a obtenu, à l'aide de cet algorithme, les congruences suivantes :

$g^{1783} \times h = 2^3 \times 3^4 \bmod p$, $g^{585} \times h = 2^7 \times 3^2 \bmod p$, $g^{726} \times h = 2^2 \times 3^5 \bmod p$, $g^{1116} \times h = 2^3 \times 3^3 \bmod p$, $g^{1393} \times h = 2^2 \times 3^6 \bmod p$.

Calculez $\log_g h$ en détaillant et en justifiant toutes les étapes.

Exercice 12 :

Soit $\mathbb{F}_5$ le corps à 5 éléments. Soit E la courbe projective d'équation $Y^2Z = X^3 + XZ^2 + 2Z^3$ sur $\mathbb{F}_5$.

Donnez la liste des points de E sur $\mathbb{F}_5$.

Montrez que le groupe $E(\mathbb{F}_5)$ des points de E sur $\mathbb{F}_5$ est cyclique.
