Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Exercices - Chapitre II

Tests et critères de primalité

Exercice 1

Soient p un nombre premier et a, r des entiers tels que $r \geq 2$ et $1 < a < p^r$. Montrer que l'on a l'équivalence

$$p^r \text{ est pseudo-premier en base } a \iff a^{p-1} \equiv 1 \text{ mod. } p^r.$$

Exercice 2

1) L'entier 341 est-il pseudo-premier ? pseudo-premier d'Euler ? pseudo-premier fort ?
2) Montrer que 561 est pseudo-premier d'Euler.
3) Soit p un nombre premier. Montrer que $3p$ n'est pas pseudo-premier.

Exercice 3 (Puissances dans un groupe cyclique)

Soient G un groupe cyclique d'ordre n, d'élément neutre e, et a un élément de G.

1) Soit $k \geq 1$ un entier. Montrer que pour qu'il existe $x \in G$ tel que $x^k = a$ il faut et il suffit que l'on ait

$$a^{\frac{n}{d}} = e \quad \text{où} \quad d = \text{pgcd}(k, n). \tag{1}$$

2) Soit $k \geq 1$ un entier tel que la condition (1) soit satisfaite. Soit x_0 un élément de G tel que $x_0^k = a$. Montrer que l'ensemble des éléments $x \in G$ tels que $x^k = a$ est

$$\Big\{x_0 z \mid z \in G \text{ et } z^d = e\Big\},$$

et que son cardinal est d. En particulier, l'équation $x^k = e$ possède exactement d solutions dans G.

Exercice 4

Soit $n \geq 3$ un entier impair composé. Posons $n - 1 = 2^s t$ où t est impair.

1) Supposons n divisible par un nombre premier congru à 3 modulo 4. Soit a un entier vérifiant les inégalités $1 < a < n$. Montrer que n est pseudo-premier fort en base a si et seulement si on a $a^t \equiv \pm 1$ mod. n.

2) Pour tout $j \geq 1$, notons p_j le j-ième nombre premier impair : on a $p_1 = 3$, $p_2 = 5, \cdots$. Soit $k \geq 2$ un entier. Supposons que n soit le produit des p_j pour j compris entre 1 et k, autrement dit que l'on ait

$$n = p_1 p_2 \cdots p_k.$$

2.1) Soit i un entier tel que $1 \leq i \leq k$. Quel est le nombre de solutions de l'équation $x^t = 1$ dans $\left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$?

2.2) En déduire l'ensemble des solutions de l'équation $x^t = 1$ dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

2.3) Quel est l'ensemble des entiers a tels que $1 < a < n$ et que n soit pseudo-premier fort en base a ?

Exercice 5

1) Soit p un nombre premier. Posons $n = 2p+1$. Montrer que n est premier si et seulement si on a $2^{n-1} \equiv 1$ mod. n.

2) Plus généralement, soient p un nombre premier et $h < p$ un entier naturel non nul. Posons $n = hp+1$ et supposons $2^h \not\equiv 1$ mod. n. Montrer n est premier si et seulement si on a $2^{n-1} \equiv 1$ mod. n.

Exercice 6

Pour tout $n \geq 1$ posons $M_n = 2^n - 1$.

1) Montrer que si n est pseudo-premier, il en est de même de M_n.

2) Soit p un nombre premier congru à 3 modulo 4. En utilisant l'exercice 5, montrer l'équivalence

$$2p+1 \text{ divise } M_p \iff 2p+1 \text{ est premier.}$$

Exercice 7 (Nombres de Carmichael)

1) Soit $n \geq 2$ un entier. Montrer que les conditions suivantes sont équivalentes :

(i) Pour tout $a \in \mathbb{Z}$, on a $a^n \equiv a$ mod. n.

(ii) Pour tout $a \in \mathbb{Z}$, premier avec n, on a $a^{n-1} \equiv 1$ mod. n.

(iii) L'entier n est sans facteurs carrés, i.e. n n'est pas divisible par le carré d'un nombre premier, et pour tout nombre premier p on a l'implication

$$p \text{ divise } n \implies p-1 \text{ divise } n-1.$$

(iv) L'entier $\lambda(n)$ divise $n-1$ où λ est la fonction de Carmichael.

Un entier n composé vérifiant l'une des conditions ci-dessus s'appelle un nombre de Carmichael.

2) Montrer que 561 et 1105 sont des nombres de Carmichael (ce sont les deux plus petits).

3) Soit n un nombre de Carmichael.

   3.1) Montrer que n est impair et possède au moins trois diviseurs premiers.

   3.2) Montrer que chaque diviseur premier de n est strictement inférieur à $\sqrt{n}$.

4) Soit $m \geq 1$ un entier. Supposons que $6m+1$, $12m+1$ et $18m+1$ soient des nombres premiers. Montrer que $(6m+1)(12m+1)(18m+1)$ est un nombre de Carmichael.

Exercice 8

Soit $n \geq 3$ un entier impair vérifiant les deux conditions suivantes :

1) Pour tout entier a premier avec n, on a $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod. n$.

2) Il existe un entier b tel que l'on ait $b^{\frac{n-1}{2}} \equiv -1 \bmod. n$.

Montrer que n est premier.

Exercice 9

Soit $n \geq 3$ un entier impair. Soit λ la fonction de Carmichael.

1) Rappeler pourquoi $\lambda(n)$ est pair.

2) Posons

$$S = \left\{ a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{\frac{\lambda(n)}{2}} = \pm 1 \right\}.$$

Montrer que $S = (\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si n est une puissance d'un nombre premier.

Exercice 10

Soient $h \geq 1$ et $N \geq 2$ des entiers naturels tels que l'on ait

$$h < 2^N \quad \text{et} \quad h \not\equiv 0 \bmod. 3.$$

Posons $n = h2^N + 1$.

1) En distinguant deux cas suivant la parité de N, calculer le symbole de Legendre $\left(\frac{n}{3}\right)$.

2) Que vaut le symbole de Jacobi $\left(\frac{3}{n}\right)$?

3) En utilisant le critère primalité de Proth, en déduire l'équivalence suivante :

$$n \text{ est premier} \iff 3^{\frac{n-1}{2}} \equiv -1 \bmod. n.$$

4) Supposons n composé et $n \not\equiv 0 \bmod. 3$. Expliciter un témoin d'Euler pour n.

Exercice 11 (Critère de primalité de Proth généralisé)

Soient p un nombre premier et h, N des entiers naturels non nuls tels que $h < p^N$. Posons
$$n = hp^N + 1.$$
Soit a un entier tel que $1 \leq a \leq n-1$ et que
$$a^{\frac{n-1}{p}} \not\equiv 1 \text{ mod. } n.$$
Notons $\Phi_p \in \mathbb{Z}[X]$ le p-ième polynôme cyclotomique. Rappelons que l'on a
$$\Phi_p = \sum_{i=0}^{p-1} X^i.$$
L'objectif de cet exercice est d'établir l'équivalence suivante :

$$(1) \qquad n \text{ est premier } \iff \Phi_p\big(a^{\frac{n-1}{p}}\big) \equiv 0 \text{ mod. } n.$$

C'est une généralisation du critère de primalité de Proth (corollaire 2.4 du cours).

1) Supposons n premier. Montrer que l'on a $\Phi_p\big(a^{\frac{n-1}{p}}\big) \equiv 0$ mod. n.

   Inversement, supposons $\Phi_p\big(a^{\frac{n-1}{p}}\big) \equiv 0$ mod. n. Posons $b = a^h$.

2) Montrer que l'on a $b^{p^N} \equiv 1$ mod. n.

   Supposons n non premier. Il existe un diviseur premier q de n plus petit que $\sqrt{n}$.

3) Montrer que p^N est l'ordre de b modulo q.
4) En déduire que l'on a $p^N < q$, puis une contradiction et l'équivalence (1).
5) Supposons n premier. Quelle est la probabilité pour qu'un entier a choisi au hasard entre 1 et $n-1$ vérifie la condition $a^{\frac{n-1}{p}} \not\equiv 1$ mod. n ?
6) Si vous disposez d'un logiciel de calculs, vérifier que les entiers
$$2.3^{1454} + 1 \quad \text{et} \quad 4.7^{894} + 1,$$
sont des nombres premiers. Ils possèdent respectivement 695 et 757 chiffres décimaux.

Exercice 12 (**Généralisation du petit théorème de Fermat**)

Soient $A \in \mathbb{M}_n(\mathbb{Z})$ une matrice de taille (n, n) à coefficients dans $\mathbb{Z}$ et p un nombre premier. Notons $\mathrm{Tr}(A)$ la trace de A. Montrer que l'on a
$$\mathrm{Tr}(A^p) \equiv \mathrm{Tr}(A) \text{ mod. } p.$$

Exercice 13

Soit $k > 1$ un entier. Montrer qu'il existe une infinité de nombres premiers p tels que $2^p - k$ soit composé.

Indication : Supposons $k > 3$ impair. Il existe un diviseur premier $q \geq 3$ de $k-2$. Utiliser alors le fait qu'il existe une infinité de nombres premiers congrus à 1 modulo $q-1$. (C'est un cas particulier du théorème de la progression arithmétique de Dirichlet.)

Exercice 14

Soit k un entier relatif distinct de 1. On se propose d'établir qu'il existe une infinité d'entiers n tels que $2^{2^n} + k$ soit composé ; cet énoncé a été démontré par le mathématicien Polonais Schinzel il y a environ 60 ans.

Indication : On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n} + k$ soit composé et que $2^{2^n} + k > a$. Puisque k est distinct de 1, il existe $s \in \mathbb{N}$ et un entier impair h tels que $k - 1 = 2^s h$. Soit t un entier naturel tel que l'on ait $p = 2^{2^t} + k > a$ et $t > s$. On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que $p - 1 = 2^s h_1$.

Soit φ la fonction indicatrice d'Euler. Montrer que l'on a $2^{2^{t+\varphi(h_1)}} + k \equiv 0 \text{ mod. } p$ et en déduire le résultat.

Exercice 15

Soit p un nombre premier. Posons

$$\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X],$$

1) Soit $m \geq 1$ un entier divisible par p. Soit q un diviseur premier de $\Phi_p(m)$.

   1.1) Montrer que q ne divise pas $m - 1$.

   1.2) En déduire que l'on a $q \equiv 1 \text{ mod. } p$.

2) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo p.

   Indication : Supposer qu'il n'existe qu'un nombre fini de nombres premiers $p_1, \cdots, p_r$ congrus à 1 modulo p, et considérer l'entier $\Phi_p(p_1 \cdots p_r p)$ afin d'obtenir une contradiction.

Exercice 16

On se propose de démontrer que pour tout nombre premier $p \geq 5$, on a la congruence

$$(1) \qquad \binom{2p-1}{p-1} \equiv 1 \text{ mod. } p^3.$$

Ce résultat a été établi par le mathématicien anglais Wolstenholme en 1862.

Posons

$$F = \prod_{k=1}^{p-1} (X - k) \in \mathbb{Z}[X],$$

et pour tout i tel que $1 \leq i \leq p-1$, notons $A_i \in \mathbb{Z}$ la i-ème fonction symétrique élémentaire des racines de F.

1) Démontrer l'égalité

$$p^{p-2} - A_1 p^{p-3} + A_2 p^{p-4} + \cdots - A_{p-2} = 0.$$

2) En déduire que l'on a

$$\prod_{k=1}^{p-1} (p+k) = 2\big(p^{p-1} + A_2 p^{p-3} + \cdots + A_{p-3} p^2\big) + A_{p-1}.$$

3) En déduire la congruence (1).

On ne connaît pas d'entiers n composés tels que $\binom{2n-1}{n-1} \equiv 1 \text{ mod. } n^3$, d'où la question suivante : pour tout $n \geq 5$, a-t-on l'équivalence

$$\binom{2n-1}{n-1} \equiv 1 \text{ mod. } n^3 \Longleftrightarrow n \text{ est premier } \;?$$

Exercice 17 (Test de Lucas des nombres de Mersenne)

Pour tout nombre premier p, posons $M_p = 2^p - 1$.

On se propose dans cet exercice de démontrer le test de Lucas (voir la remarque 2.8 du cours) : soit $(u_n)_{n\geq 1}$ la suite d'entiers définie par les conditions

$$u_1 = 4 \quad \text{et} \quad u_{n+1} = u_n^2 - 2.$$

Soit $p \geq 3$ un nombre premier. On a l'équivalence

$$(1) \qquad M_p \text{ est premier } \Longleftrightarrow u_{p-1} \equiv 0 \text{ mod. } M_p.$$

1. Préliminaires

Soit $A = \mathbb{Z}\big[\sqrt{3}\big]$ le sous-anneau de $\mathbb{C}$ engendré par 1 et $\sqrt{3}$ (une racine carrée de 3). C'est l'ensemble des éléments de la forme $a + b\sqrt{3}$ où a et b sont dans $\mathbb{Z}$. Posons

$$u = 2 + \sqrt{3}, \quad u' = 2 - \sqrt{3}, \quad z = 1 + \sqrt{3}, \quad z' = 1 - \sqrt{3}.$$

On a les égalités

$$u+u'=4, \quad uu'=1, \quad z+z'=2, \quad zz'=-2, \quad z^2=2u.$$

1) Vérifier que pour tout $n \geq 1$, on a

$$u_n = u^{2^{n-1}} + u'^{2^{n-1}}.$$

2) Soit q un nombre premier. Montrer que les anneaux A/qA et $\mathbb{F}_q[X]/(X^2-3)$ sont isomorphes.

2. Preuve de la nécessité

Supposons que M_p soit premier. Posons

$$q = M_p \quad \text{et} \quad K = A/qA.$$

Notons x, η, η', y, y' les classes modulo qA respectivement de $\sqrt{3}$, u, u', z et z'.

3) Montrer que 3 n'est pas un carré modulo q et que K est un corps à q^2 éléments.

On identifie $\mathbb{F}_q$ à un sous-corps de K.

4) Soit $f : K \to K$ l'automorphisme de Frobenius de K, défini pour tout $t \in K$ par l'égalité $f(t) = t^q$. Quels sont les points fixes de f ? Vérifier que l'on a

$$f(x) = -x, \quad f(\eta) = \eta' \quad \text{et} \quad f(y) = y'.$$

5) En déduire les égalités $\eta^{\frac{q+1}{2}} = \eta'^{\frac{q+1}{2}} = -1$.
6) En déduire que l'on a $\left(\eta^{\frac{q+1}{4}} + \eta'^{\frac{q+1}{4}}\right)^2 = 0$, puis que q divise u_{p-1}.

3. Preuve de l'implication réciproque

Supposons que M_p divise u_{p-1}. Procédons par l'absurde en supposant que M_p n'est pas premier. Il existe alors un diviseur premier q de M_p tel que $q^2 \leq M_p$. Posons de nouveau $K = A/qA$ et notons η, η' les classes de u et u' modulo qA.

7) Montrer l'égalité $\eta^{2^{p-2}} + \eta'^{2^{p-2}} = 0$.
8) En déduire que η est d'ordre 2^p dans le groupe des éléments inversibles de K (dans cette question K n'est pas nécessairement un corps).
9) En déduire une contradiction, puis l'équivalence (1).

Exercice 18

Soit $(u_n)_{n \in \mathbb{N}}$ la suite d'entiers définie par les égalités

$$u_0 = 0, \quad u_1 = 1 \quad \text{et} \quad u_n = u_{n-1} + u_{n-2} \quad \text{pour tout } n \geq 2.$$

C'est la suite de Fibonacci. Soit p un nombre premier. L'objectif de cet exercice est de prouver que p divise u_{p-1} si $p \equiv \pm 1$ mod. 5 et que p divise u_{p+1} si $p \equiv \pm 2$ mod. 5.

Soit p un nombre premier distinct de 5. Considérons l'anneau quotient

$$A = \mathbb{F}_p[X]/(f) \quad \text{où} \quad f = X^2 - X - 1 \in \mathbb{F}_p[X].$$

Identifions $\mathbb{F}_p$ à un sous-anneau de A et notons α la classe de X modulo (f).

1. Questions préliminaires

1) Calculer le symbole de Legendre $\left(\frac{5}{p}\right)$.
2) Montrer que α et $1-\alpha$ sont inversibles dans A.
3) Montrer que $2\alpha - 1$ est inversible dans A.
4) Montrer que pour tout $n \in \mathbb{N}$, on a

$$u_n + p\mathbb{Z} = \frac{\alpha^n - (1-\alpha)^n}{2\alpha - 1}.$$

2. Cas où $p \equiv \pm 1$ mod. 5

5) Montrer que A est isomorphe à l'anneau produit $\mathbb{F}_p \times \mathbb{F}_p$.
6) Montrer que pour tout $x \in A$, on a $x^p = x$.
7) En déduire la congruence $u_{p-1} \equiv 0$ mod. p.

3. Cas où $p \equiv \pm 2$ mod. 5

8) Montrer que A est un corps.
9) Quelles sont les racines du polynôme F dans A ?
10) Montrer que l'on a $\alpha^p = 1 - \alpha$ et $(1-\alpha)^p = \alpha$.
11) En déduire la congruence $u_{p+1} \equiv 0$ mod. p.