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

Correction des exercices - Chapitre III

Méthodes de factorisation

Exercice 1

1) On trouve $k = 2^3 \times 3^2 \times 5 \times 7 \times 11 = 27720$.

2) On écrit le développement de k en base 2. On vérifie que l'on a

$$k = 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^6 + 2^3.$$

On peut ainsi déterminer 2^k modulo n avec dix-neuf multiplications. On a

$$2^{2^3} = 256, \quad 2^{2^4} = 256^2 = 65536, \quad 2^{2^5} \equiv 333960 \text{ mod. } n,$$

$$2^{2^6} \equiv 162174 \text{ mod. } n, \quad 2^{2^{10}} \equiv 422420 \text{ mod. } n, \quad 2^{2^{11}} \equiv 369858 \text{ mod. } n,$$

$$2^{2^{13}} \equiv 311527 \text{ mod. } n, \quad 2^{2^{14}} \equiv 357679 \text{ mod. } n.$$

On en déduit que 114354 est le reste cherché i.e. que l'on a

$$2^k \equiv 114354 \text{ mod. } n.$$

3) En utilisant l'algorithme d'Euclide, on en déduit que l'on a

$$\text{pgcd}(2^k - 1, n) = \text{pgcd}(n, 114353) = 661.$$

4) La factorisation de n en produits de nombres premiers est donc $n = 641 \times 661$.
On notera que l'algorithme considéré fonctionne ici car $660 = 2^2 \times 3 \times 5 \times 11$ est un produit de puissances de nombres premiers inférieures ou égales à celles intervenant dans la décomposition de k.

Exercice 2

1) Factorisons l'entier 247. Les trois premiers termes de la suite $(x_i)_{i \in \mathbb{N}}$ définie par les égalités

$$x_0 = 3 \quad \text{et} \quad x_{i+1} = f(x_i) \text{ mod. } 247$$

sont $x_0 = 3$, $x_1 = 10$ et $x_2 = 101$. On a $\text{pgcd}(x_2 - x_1, 247) = 13$, d'où $247 = 13 \times 19$.

En ce qui concerne l'entier 481, on calcule les premiers termes de la suite $(x_i)_{i\in\mathbb{N}}$ définie par $x_0 = 3$ et l'égalité $x_{i+1} = f(x_i)$ mod. 481. On a

$$x_0 = 3, \quad x_1 = 10, \quad x_2 = 101.$$

L'égalité $\text{pgcd}(x_2 - x_1, 481) = 13$ implique alors l'égalité $481 = 13 \times 37$.

2) Posons $n = 6059$. La partie entière de $\sqrt{n}$ est 77. On a $(77+1)^2 - n = 5^2$, d'où $n = 78^2 - 5^2$. On obtient $n = 73 \times 83$.

Exercice 3

1) On a les égalités

$$2N = m^r + m - 2 = (m^r - 1) + (m - 1).$$

On en déduit que $m-1$ divise $2N$. L'entier m étant pair, $m-1$ divise N. On a $m-1 \neq 1$ car m est au moins 4. De plus, on a $m-1 \neq N$. En effet, l'égalité $m-1 = N$ implique $m = m^r$, puis $r = 1$, or r est au moins 2, d'où l'assertion.

2) On a

$$2^{64} + 15 = \frac{(2^5)^{13}}{2} + \frac{2^5}{2} - 1.$$

La question précédente, utilisée avec l'entier $m = 2^5$, entraîne que $2^{64}+15$ est divisible par 31.

Exercice 4

1) Supposons n composé. Il existe deux entiers $a > 1$ et $b > 1$ tels que l'on ait $n = ab$. Par ailleurs, on a l'égalité

$$R_n = \frac{10^n - 1}{9}.$$

On a ainsi

$$R_n = \frac{10^{ab} - 1}{9} = \frac{10^{ab} - 1}{10^a - 1} \times \frac{10^a - 1}{9},$$

et R_n est donc le produit de deux entiers strictement plus grands que 1, autrement dit, R_n n'est pas premier, d'où le résultat.

Les seules valeurs de n pour lesquelles on sache que R_n est premier sont $2, 19, 23, 317$ et 1031. Il est probable que pour $n = 49081, 86453, 109297, 270343$, R_n soit premier.

2) Pour $p = 3$, les entiers R_n avec n multiple de 3 conviennent. Supposons $p \geq 7$. On a alors $10^{p-1} \equiv 1$ mod. p, d'où pour tout $k \in \mathbb{N}$, la congruence $10^{k(p-1)} \equiv 1$ mod. p. Parce que $p \neq 3$, on obtient

$$R_{k(p-1)} = \frac{10^{k(p-1)} - 1}{9} \equiv 0 \text{ mod. } p,$$

d'où le résultat. Notons que R_n n'est pas multiple de 5 si $n \geq 1$, car on a $9R_n = 10^n - 1$.

3) On a $10^n \equiv 1$ mod. ℓ. Soit d l'ordre multiplicatif de 10 modulo ℓ (10 est inversible modulo ℓ). Par hypothèse on a $n \geq 5$, donc ℓ est distinct de 3. Par suite, on a $d \neq 1$, d'où $d = n$. Il en résulte que n divise $\ell - 1$. Puisque $\ell - 1$ est pair et que n est distinct de 2, l'entier $2n$ divise $\ell - 1$, d'où l'assertion.

4) En utilisant la question précédente, recherchons un diviseur premier de cet entier. Il n'est pas divisible par 11. On constate ensuite qu'il ne l'est pas par 31, mais qu'il est divisible par 41. On vérifie alors que la décomposition cherchée est

$$R_5 = 41 \times 271.$$

Exercice 5

Démontrons que l'ensemble cherché est $\{1, 2, 3, 8\}$.

Si $n \in \{1, 2, 3, 8\}$, alors $n(n+1)$ est 3-friable.

Inversement, soit $n \geq 2$ un entier tel que $n(n+1)$ soit 3-friable. Parce que n et $n+1$ sont premiers entre eux, l'un de ces entiers est une puissance de 2 et l'autre est une puissance de 3. On est donc amené à distinguer les deux cas suivants.

1) Supposons qu'il existe a et b tels que $n = 2^a$ et $n + 1 = 3^b$. On a ainsi l'égalité

$$3^b - 2^a = 1.$$

On a $n \geq 2$, d'où $a \geq 1$. Si $a = 1$, on obtient $n = 2$.

Supposons $a \geq 2$. On a

$$3^b \equiv (-1)^b \equiv 1 \text{ mod. } 4,$$

donc b est pair. Posons $b = 2c$. On a ainsi $(3^c - 1)(3^c + 1) = 2^a$. Il existe donc des entiers u et v (de somme a) tels que l'on ait

$$3^c - 1 = 2^u \quad \text{et} \quad 3^c + 1 = 2^v.$$

Par ailleurs on a $c \geq 1$, d'où $3^c + 1 \geq 4$ puis $v \geq 2$, ce qui entraîne la congruence

$$3^c \equiv -1 \text{ mod. } 4.$$

Il en résulte que $3^c - 1 \equiv 2$ mod. 4, d'où $u = 1$. On obtient alors $c = 1$, ce qui conduit à $n = 8$.

2) Supposons qu'il existe a et b tels que $n = 3^a$ et $n + 1 = 2^b$. Dans ce cas, on a $b \geq 1$ et

$$2^b - 3^a = 1.$$

On a en particulier

$$2^b \equiv (-1)^b \equiv 1 \text{ mod. } 3.$$

Il existe donc $c \geq 1$ tel que $b = 2c$. On obtient l'égalité

$$(2^c - 1)(2^c + 1) = 3^a,$$

d'où l'existence d'entiers u et v, avec $u < v$, tels que l'on ait

$$2^c - 1 = 3^u \quad \text{et} \quad 2^c + 1 = 3^v.$$

Parce que $2^c - 1$ et $2^c + 1$ sont premiers entre eux, on en déduit que $u = 0$. On obtient alors $c = 1$, puis $n = 3$, d'où le résultat.

Exercice 6 (Carrés modulo p^r)

1) Soit $f : G \to G$ l'application définie par $f(x) = x^2$. C'est un homomorphisme de groupes. Le groupe G étant cyclique d'ordre pair, il possède un unique élément d'ordre 2. Ainsi le noyau de f est d'ordre 2 et son image, qui est l'ensemble des carrés de G, est d'ordre $\frac{n}{2}$. Parce que G est cyclique, il existe un unique sous-groupe d'ordre $\frac{n}{2}$ de G. Il est formé des éléments x tels que $x^{\frac{n}{2}}$ soit l'élément neutre, d'où le résultat.

2.1) Démontrons la congruence annoncée par récurrence. On a

$$(1 + pa)^p = \sum_{k=0}^{p} \binom{p}{k} (pa)^k \equiv 1 + p^2 a + \binom{p}{2} (pa)^2 \text{ mod. } p^3.$$

Parce que $p \neq 2$, l'entier $\binom{p}{2}$ est divisible par p, d'où

$$(1 + pa)^p \equiv 1 + p^2 a \text{ mod. } p^3,$$

et la formule est vraie pour $n = 1$. Soit alors $n \geq 1$ un entier tel qu'elle soit vraie pour l'entier n. Il existe $b \in \mathbb{Z}$ tel que l'on ait

$$(1 + pa)^{p^n} = 1 + p^{n+1} a + p^{n+2} b.$$

Par suite, on a

$$(1 + pa)^{p^{n+1}} = (1 + p^{n+1}(a + pb))^p \equiv 1 + p^{n+2} a \text{ mod. } p^{n+3},$$

d'où le résultat.

2.2) Soit $r \geq 1$ un entier. Par hypothèse n est un carré non nul modulo p. D'après le critère d'Euler, on a donc

$$n^{\frac{p-1}{2}} \equiv 1 \text{ mod. } p.$$

Autrement dit, il existe $a \in \mathbb{Z}$ tel que l'on ait $n^{\frac{p-1}{2}} = 1 + pa$. D'après la question précédente, on a donc

$$n^{\frac{p^{r-1}(p-1)}{2}} = (1+pa)^{p^{r-1}} \equiv 1 + p^r a \text{ mod. } p^{r+1},$$

d'où

$$n^{\frac{p^{r-1}(p-1)}{2}} \equiv 1 \text{ mod. } p^r.$$

Parce que p est impair, le groupe $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ est cyclique d'ordre $p^{r-1}(p-1)$. La question 1 entraîne alors le résultat.

Exercice 7

Reprenons la méthode présentée dans le paragraphe 6 du cours, avec l'entier $B = 7$. Posons $Q(X) = X^2 - n \in \mathbb{Z}[X]$. On a $\sqrt{n} \simeq 50,7$. On est donc amené à rechercher suffisamment d'entiers x dans un intervalle de la forme $[51, 51 + A]$ tels que $Q(x)$ soit 7-friable. On vérifie que l'on a $Q(51) = 28 = 4 \times 7$ et $Q(54) = 343 = 7^3$. On obtient $Q(51)Q(54) = 2^2 \times 7^4$ qui est un carré. On en déduit la congruence (condition (9) du chapitre III)

$$(51 \times 54)^2 \equiv 2^2 \times 7^4 \text{ mod. } n,$$

autrement dit,

$$2754^2 \equiv 98^2 \text{ mod. } n.$$

On a $\text{pgcd}(2754 - 98, n) = 83$, d'où l'égalité $n = 31 \times 83$.

Exercice 8 (Nombres de Fermat)

1) Soit p un facteur premier de F_n. On a $2^{2^n} \equiv -1$ mod. p et $2^{2^{n+1}} \equiv 1$ mod. p. Par suite, l'ordre de 2 modulo p est 2^{n+1}. D'après le théorème de Lagrange, 2^{n+1} divise $p - 1$. En particulier, on a $p \equiv 1$ mod. 8, d'où $\left(\frac{2}{p}\right) = 1$. D'après le critère d'Euler, on obtient

$$2^{\frac{p-1}{2}} \equiv 1 \text{ mod. } p,$$

donc 2^{n+1} divise $\frac{p-1}{2}$, d'où l'assertion.

2) Cette démonstration est due à Euler. Posons $p = 641$. On a les égalités

$$p = 5^4 + 2^4 = 5.2^7 + 1.$$

Par suite, on a $5.2^7 \equiv -1$ mod. p, d'où $5^4.2^{28} \equiv 1$ mod. p, puis $-2^{32} \equiv 1$ mod. p, autrement dit on a $F_5 \equiv 0$ mod. p.
On en déduit l'égalité

$$F_5 = 641 \times 6700417,$$

qui est la décomposition en facteurs premiers de F_5.

3) Soit d l'ordre multiplicatif de 2 modulo p. L'entier d divise $p-1$. Il existe des entiers a et h tels que l'on ait $2^d = 1 + ap$ et $p - 1 = dh$. On obtient

$$2^{p-1} = 2^{dh} = (1 + ap)^h \equiv 1 + ahp \text{ mod. } p^2.$$

D'après l'hypothèse faite, p divise donc a. Par suite, on a $2^d \equiv 1$ mod. p^2. L'entier d divise m, d'où le résultat.

4) Supposons que p^2 divise F_n. On a $2^{2^n} \equiv -1$ mod. p^2, d'où $2^{2^{n+1}} \equiv 1$ mod. p^2. Pour tout $k \in \mathbb{N}$, on a donc $2^{k2^{n+1}} \equiv 1$ mod. p^2. D'après la question 1, il existe k tel que $p = 1 + k2^{n+1}$, d'où $2^{p-1} \equiv 1$ mod. p^2.
Inversement, supposons $2^{p-1} \equiv 1$ mod. p^2. On a $2^{2^n} \equiv -1$ mod. p, d'où la congruence $2^{2^{n+1}} \equiv 1$ mod. p. D'après la question précédente, on en déduit que l'on a

$$2^{2^{n+1}} \equiv 1 \text{ mod. } p^2.$$

Ainsi p^2 divise $(2^{2^n} - 1)(2^{2^n} + 1)$. Les entiers $2^{2^n} - 1$ et $2^{2^n} + 1$ étant premiers entre eux et p divisant F_n, il en résulte que p^2 divise F_n.

5) Supposons qu'il existe une infinité de nombres de Fermat divisibles par le carré d'un nombre premier. Parce que deux nombres de Fermat distincts sont premiers entre eux (si $n > m$ on a $F_n \equiv 2$ mod. F_m, voir la page 5 du chapitre II), on obtient alors l'assertion 5.2.

Exercice 9

Soit A un entier qui soit le produit de n entiers consécutifs. On peut supposer $A \geq 1$. Il existe $k \in \mathbb{N}$ tel que l'on ait

$$A = \prod_{i=1}^{n} (k + i).$$

Le coefficient binomial $\begin{pmatrix} k+n \\ k \end{pmatrix}$ est un entier et on a les égalités

$$\begin{pmatrix} k+n \\ k \end{pmatrix} = \frac{(k+n)!}{k!n!} = \frac{A}{n!},$$

par suite A est divisible par $n!$.

Exercice 10

On peut supposer qu'il existe $n_0 \in \mathbb{N}$ tel que $p = |f(n_0)|$ soit premier. Parce que f est non constant la limite de $|f(x)|$ quand x tend vers $+\infty$ est $+\infty$. Il existe donc n_1 tel que pour tout $n \geq n_1$ on ait $|f(n)| > p$. Pour tout entier $h \geq 1$ on a

$$f(n_0 + ph) = f(n_0) + pr \quad \text{où} \quad r \in \mathbb{Z}.$$

Le nombre premier p divise $f(n_0+ph)$. Pour tout h tel que $n_0+ph \geq n_1$, on a $|f(n_0+ph)| > p$, donc $|f(n_0+ph)|$ est composé, d'où le résultat.

Exercice 11

1) Si f a une racine $n \in \mathbb{Z}$, on a $f(n)=0$, donc tous les nombres premiers divisent $f(n)$.
2) Parce que f est distinct de ± 1, les polynômes $f-1$ et $f+1$ n'ont qu'un nombre fini de racines. Il existe donc $n \in \mathbb{Z}$ tel que $f(n)$ soit distinct de ± 1. L'entier $f(n)$ est divisible par un nombre premier qui, par définition, est dans $P(f)$.
3) C'est une conséquence de la première question et de l'hypothèse faite sur $P(f)$.
4) Posons $f = c + a_1X + \cdots + a_nX^n$. On a

$$f\big(rcX\big) = c + \sum_{i=1}^{n} a_i(rcX)^i = c\Big(1 + \sum_{i=1}^{n} a_i c^{i-1} r^i X^i\Big),$$

de sorte que pour tout $i = 1, \cdots, n$, l'entier $b_i = a_i c^{i-1} r^i$ convient.

5) Posons $g = 1 + b_1X + \cdots + b_nX^n$. Puisque c est non nul, on a $b_n \neq 0$, donc g est de degré n, et en particulier on a $g \neq \pm 1$. D'après la question 2, il existe un nombre premier p qui divise g. C'est aussi un diviseur premier de f (question 4). Par suite, p divise r. Les entiers b_i sont donc divisibles par p. Cela entraîne que p divise 1, d'où une contradiction et le résultat.

6.1) Si 541 était composé, il serait divisible par un nombre premier inférieur ou égal à 23, et on vérifie que ce n'est pas le cas. D'après la loi de réciprocité quadratique, on a

$$\Big(\frac{13}{541}\Big) = \Big(\frac{541}{13}\Big) = \Big(\frac{8}{13}\Big) = \Big(\frac{2}{13}\Big)^3 = -1.$$

6.2) Le discriminant du polynôme f est 13. Parce que 13 n'est pas un carré modulo 541, il en résulte que 541 n'appartient pas à $P(f)$.

7.1) Rappelons que dans $\mathbb{Z}[X]$ on a l'égalité

$$X^n - 1 = \prod_{k|n} \Phi_k. \tag{1}$$

Notons d l'ordre de a modulo p.

Supposons que p divise $\Phi_n(a)$. D'après (1), on a $a^n \equiv 1$ mod. p. On en déduit que p ne divise pas a et que d divise n. Supposons que l'on ait $d < n$. On a $a^d \equiv 1$ mod. p et d'après (1) il existe donc un diviseur r de d tel que p divise $\Phi_r(a)$. On a $r \neq n$ et r divise n, d'où $a^n \equiv 1$ mod. p^2. Par ailleurs, on a

$$\Phi_n(a+p) \equiv \Phi_n(a) \text{ mod. } p \quad \text{et} \quad \Phi_r(a+p) \equiv \Phi_r(a) \text{ mod. } p,$$

donc p divise $\Phi_n(a+p)$ et $\Phi_r(a+p)$. D'après (1), on a ainsi $(a+p)^n \equiv 1$ mod. p^2. On obtient

$$(a+p)^n - 1 = a^n + npa^{n-1} - 1 \equiv 0 \text{ mod. } p^2.$$

Vu que $a^n \equiv 1$ mod. p^2, le nombre premier p divise an, ce qui d'après l'hypothèse faite conduit à une contradiction. On a donc $d = n$.
Inversement, supposons $d = n$. On a $a^n \equiv 1$ mod. p. Il existe donc un diviseur r de n tel que p divise $\Phi_r(a)$ (égalité (1)). Parce que $\Phi_r(a)$ divise $a^r - 1$ on en déduit que $a^r \equiv 1$ mod. p, donc n divise r, puis $n = r$. Ainsi p divise $\Phi_n(a)$.

7.2) Supposons $p \equiv 1$ mod. n. Le groupe $\mathbb{F}_p^*$ est cyclique, donc il existe un élément d'ordre n dans $\mathbb{F}_p^*$ i.e. il existe $a \in \mathbb{Z}$, non divisible par p, d'ordre n modulo p. Il en résulte que $\Phi_n(a) \equiv 0$ mod. p i.e. que p divise Φ_n (question 7.1).

Inversement, supposons que Φ_n possède une racine a modulo p. Alors, n est l'ordre de a modulo p (*loc. cit.*). On a $a^n \equiv 1$ mod. p. Parce que p ne divise pas a, on a $a^{p-1} \equiv 1$ mod. p, donc n divise $p - 1$.

8) D'après la question 5, l'ensemble $P(\Phi_n)$ est infini, d'où l'assertion (question 7.2).

9) Il existe au moins un tel entier n, à savoir $n = 2$. Par ailleurs, pour tout $n \geq 1$, on a

$$(n^5)^2 + 1 = \Phi_5(-n^2)(n^2 + 1).$$

D'après la question 7.2, tout diviseur premier, distinct de 5, de $\Phi_5(-n^2)$ est congru à 1 modulo 5. Il en résulte que si n est un entier satisfaisant la propriété qui figure dans l'énoncé, il en est de même de n^5, d'où le résultat.