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

Exercices - Chapitre III

Méthodes de factorisation

Exercice 1

L'objectif de cet exercice est de trouver la décomposition en facteurs premiers de l'entier $n = 423701$ en utilisant méthode $p-1$ de Pollard. Il est préférable d'utiliser une calculatrice pour la résolution de cet exercice.

1) Trouver le plus petit commun multiple k de tous les entiers inférieurs ou égaux à 12.
2) Déterminer le reste de la division euclidienne de 2^k par n.
3) Calculer le pgcd de $2^k - 1$ et n.
4) En déduire la factorisation de n.

Exercice 2

1) Factoriser les entiers 247 et 481 avec la méthode rho de Pollard, en utilisant le couple (f, x_0) où $f = X^2 + 1 \in \mathbb{Z}[X]$ et $x_0 = 3$.
2) Factoriser l'entier 6059 par la méthode de Fermat.

Exercice 3

Soient $m \geq 4$ un entier pair et $r \geq 2$ un entier. Posons

$$N = \frac{m^r}{2} + \frac{m}{2} - 1.$$

1) Montrer que N est un entier composé en explicitant un diviseur de N.
2) En déduire que $2^{64} + 15$ est divisible par 31.

   On peut facilement vérifier avec la méthode des divisions successives que $\frac{2^{64}+15}{31}$ est divisible par 107. On obtient $2^{64} + 15 = 31 \times 107 \times 5561273462077043$, qui est un produit de trois nombres premiers.

Exercice 4

Pour tout $n \geq 1$, considérons l'entier $R_n = 1 \cdots 1$ constitué de n chiffres 1.

1) Montrer si R_n est premier, alors n est premier.

2) Soit p un nombre premier impair distinct de 5. Montrer qu'il existe une infinité d'entiers n tels que R_n soit divisible par p.

3) Supposons $n \geq 5$ premier. Soit ℓ un diviseur premier de R_n. Montrer que ℓ est congru à 1 modulo $2n$.

4) En déduire que R_5 est composé, ainsi que sa décomposition en facteurs premiers.

Exercice 5

Rappelons qu'un entier est dit B-friable si tous ses diviseurs premiers sont inférieurs ou égaux à B. Déterminer l'ensemble des entiers $n \geq 1$ tels que $n(n+1)$ soit 3-friable.

Exercice 6 (Carrés modulo p^r)

1) Soit G un groupe cyclique d'ordre n pair. Pour tout $x \in G$, montrer que x est un carré dans G si et seulement si $x^{\frac{n}{2}}$ est l'élément neutre de G.

2) Soit p un nombre premier impair.

2.1) Soient a et n des entiers avec $n \geq 1$. Montrer que l'on a

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

2.2) Supposons n non divisible par p et que n soit un carré modulo p. En déduire que pour tout $r \geq 1$, n est un carré modulo p^r.

Exercice 7

Posons $n = 2573$. Déterminer la décomposition en facteurs premiers de n, en utilisant la méthode de recherche de congruences de carrés, avec l'entier $B = 7$.

Exercice 8 (Nombres de Fermat)

Pour tout $n \in \mathbb{N}$, posons $F_n = 2^{2^n} + 1$.

1) Si $n \geq 2$, montrer que chaque diviseur premier de F_n est congru à 1 modulo 2^{n+2}.

2) Montrer que 641 divise F_5.

3) Soit p un nombre premier tel que $2^{p-1} \equiv 1 \text{ mod. } p^2$. Soit m un entier naturel tel que $2^m \equiv 1 \text{ mod. } p$. Montrer que l'on a $2^m \equiv 1 \text{ mod. } p^2$.

4) Soit p un diviseur premier de F_n. Montrer que p^2 divise F_n si et seulement si on a $2^{p-1} \equiv 1 \text{ mod. } p^2$.

5) En déduire que l'une des deux assertions suivantes est vraie :

5.1) Il n'existe qu'un nombre fini de nombres de Fermat divisibles par le carré d'un nombre premier.

5.2) Il existe une infinité de nombres premiers p tels que $2^{p-1} \equiv 1 \text{ mod. } p^2$.

Exercice 9

Montrer que le produit de n entiers consécutifs est divisible par $n!$.

Exercice 10

Soit f un polynôme de $\mathbb{Z}[X]$ de degré ≥ 1. Montrer qu'il existe une infinité d'entiers $n \in \mathbb{N}$ tels que $f(n)$ soit composé.

Exercice 11

Étant donnés un polynôme $f \in \mathbb{Z}[X]$ et un nombre premier p, on dit que p est un diviseur premier de f s'il existe $n \in \mathbb{Z}$ tel que p divise $f(n)$, autrement dit si f a une racine modulo p. Notons $P(f)$ l'ensemble des diviseurs premiers de f.

On se propose d'établir que si f est non constant, $P(f)$ est infini.

1) Soit f un polynôme de $\mathbb{Z}[X]$ ayant une racine dans $\mathbb{Z}$. Montrer que tous les nombres premiers sont dans $P(f)$.
2) Pour tout $f \in \mathbb{Z}[X]$, distinct de ± 1, montrer que $P(f)$ est non vide.

Soit $f \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$. Procédons par l'absurde en supposant que $P(f)$ est fini. Notons r le produit des nombres premiers qui appartiennent à $P(f)$.

3) Montrer que $f(0)$ n'est pas nul.
4) Montrer qu'il existe des entiers relatifs $b_1, \cdots, b_n$, divisibles par r, tels que l'on ait

$$f\big(rcX\big) = c\big(1 + b_1 X + \cdots + b_n X^n\big) \quad \text{avec} \quad c = f(0).$$

5) En déduire une contradiction et le fait que $P(f)$ soit infini.
6) Posons $f = X^2 - 3X - 1 \in \mathbb{Z}[X]$.

   6.1) Montrer que 541 est premier et calculer le symbole de Legendre $\left(\frac{13}{541}\right)$.

   6.2) L'entier 541 appartient-il à $P(f)$?

Soit $n \geq 1$ un entier. Notons $\Phi_n \in \mathbb{Z}[X]$ le n-ième polynôme cyclotomique.

7) Soit p un nombre premier ne divisant pas n.

   7.1) Soit a un entier. Montrer que p divise $\Phi_n(a)$ si et seulement si p ne divise pas a et n est l'ordre de a modulo p.

   7.2) En déduire que p divise Φ_n si et seulement si on a $p \equiv 1$ mod. n.
8) En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo n.
9) Montrer qu'il existe une infinité d'entiers n possédant la propriété suivante : soit p un diviseur premier de $n^2 + 1$. Alors, on a $p = 5$ ou $p \equiv 1$ mod. 5.