105 Exercices illustrant l'utilisation de nombres premiers

Exercice 1

1°/ Soit $k \in \mathbb{N}^*$. Montrer que si $2^k + 1$ est premier alors k est une puissance de 2.

Les nombres $f_n = 2^{2^n} + 1$, $n \in \mathbb{N}$ sont appelés nombres de Fermat

2°/ a) A-t-on $\forall n \in \mathbb{N}$, f_n est premier ?

b) Montrer que les nombres $(f_n)_{n \in \mathbb{N}}$ sont premiers 2 à 2.

Exercice 2.

On se donne p, q deux nombres premiers distincts.

1°/ Justifier que pour $a \in \mathbb{Z}$ non divisible par p et q

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

2°/ Soit $e \in \{1, \dots, (p-1)(q-1)\}$ premier avec $(p-1)(q-1)$. Justifier l'existence $d \in \{1, \dots (p-1)(q-1)\}$ tq $ed \equiv 1 [(p-1)(q-1)]$

3°/ Montrer que $\forall a \in \mathbb{Z}$ $a^{ed} \equiv a \ (pq)$

4°/ Exemple trivial : soit $p = 3$, $q = 11$. On choisit $e = 20$

déterminer d, puis chiffrer le message $a = 9$

vérifier par déchiffrement que l'on retrouve le message

Exercice 3 Soit p nombre premier.

1) Soit G groupe abélien, si $x_1, x_2 \in G$ d'ordre respectifs p_1 et p_2 avec $p_1 \wedge p_2 = 1$,

Montrer que l'ordre de $x_1 x_2$ est $p_1 p_2$.

(On acceptera la généralisation pour $x_1, \dots x_r$ d'ordre $p_1, \dots p_r$ avec les p_i étant 2 à 2 premiers).

2) Soit q un nombre premier tel que $q \mid p-1$. Etablir l'existence d'un élément $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ d'ordre multiplicatif q.

3) q un nombre premier et $\alpha \in \mathbb{N}^*$ tels que $q^\alpha \mid p-1$. Montrer l'existence d'un élément de $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ d'ordre q^α.

4) En déduire $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ est cyclique.

Exercice 4. Soit n entier ≥ 2

on note $\varphi(n) = \text{card}\{1 \leq p \leq n \mid p \wedge n = 1\}$

et $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition de n en produit de facteurs premiers.

Le but est de montrer que $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$ (*)

On tire au hasard 1 entre copies entre 1 et n. On note

A « le nombre obtenu est premier avec n »

et $\forall i \in [\![1, k]\!]$ A_i : « le nombre obtenu est divisible par p_i »

1°/ Définir l'espace probabilisé modélisant l'épreuve

2°/ Exprimer $P(A)$ en fonction de $\varphi(n)$ et n

3°/ Montrer que $\forall i \in [\![1, k]\!]$ $P(A_i) = \frac{1}{p_i}$

4°/ Montrer que les événements $A_1, \dots A_k$ sont indépendants

5°/ Exprimer A en fonction des A_i et déduire la relation (*)

→ 1) def de n -

2) décomposition d'un nombre entier n en produit de facteurs premiers

$n = \prod_{i=1}^{q} p_i^{d_i}$ $\quad p_i \in \mathcal{P}$ et $d_i \in \mathbb{N}^*$.

3) Corps $\mathbb{Z}/p\mathbb{Z}$ p premier

$p \in \mathbb{N}^*$, 3 propriétés équivalentes

1) p premier

2) $\mathbb{Z}/p\mathbb{Z}$ est 1 corps

3) $\mathbb{Z}/p\mathbb{Z}$ anneau intègre

5) petit théorème de fermat

p nombre premier et $n \in \mathbb{Z}$ $\quad n^p \equiv n \ (p)$

et si $p \nmid n$ alors $n^{p-1} \equiv 1 \ (p)$

4) Fonction indicatrice d'Euler

$\varphi(n) = \text{Card} \{ m \in [\![1, n]\!] \text{ tel que } m \wedge n = 1 \text{ et } m \neq n \}$.

Théorème d'Euler.

Soit $n \in \mathbb{N}^*$ ~~$\forall a \in (\mathbb{Z}/n\mathbb{Z})^\times$ $a^{\varphi(n)} = 1 \ (n)$~~

pour tout $a \in \mathbb{Z}$ premier avec n $\quad a^{\varphi(n)} = 1 \ (n)$

Ex 1 => nombre de fermat.

caractéristique des nombres

- conjecture historique

- (F_n) sont premiers 2 à 2.

RSA) méthode de cryptographie basée sur la notion premier
ont produit de 2 nombres premiers assez grands.
détermination

1°/ q.1, ~~attribut d'erreur~~
résultat utile par la dernière Q
repose sur th. d'Euler

$a \wedge p$, $a \wedge q$; $a \wedge pq$ donc $a^{\varphi(pq)} = 1 \ (pq)$

2°/ on choisit e premier avec $(p-1)(q-1)$, on veut trouver
son inverse modulo $(p-1)(q-1)$
→ construction de la clé privée de décryp.

3°/ On vérifie que l'on peut décrypter dans tous les cas l'envoyé

---

4) $1 \leq d \leq \frac{n}{p_i}$ ⊕ indépendance.

indep. des A_i alors indep des $\overline{A_i}$

$\mathbb{P}(A) = \mathbb{P}(\cap \overline{A_i})$
$= \prod P(\overline{A_i})$

---

p premier $\mathbb{Z}/p\mathbb{Z}$ est 1 corps

3) abelien. cyclique

G groupe fini d'ordre n
G cyclique ⟺ G possède au moins 1 élt d'ordre n.

Travail sur [l'ordre des élts]

→ travail sur nb premier
par puissance par décomp.

p premier. $x^p = 1$
$o(x) \mid p$ mais ~~p≠1~~
$o(x) = p$
$o(x) = 1$

Ex1 a) Par contraposée. k pas puissance de 2 $\Rightarrow$ k a au moins 1 facteur impair $p > 0$ dans sa décomp. première

k pas puissance de 2.

$\Rightarrow$ décomp. primale de k, il a au moins 1 facteur impair $p > 1$

$$\exists q \in \mathbb{N}^* \quad k = pq$$

alors $2^k + 1 = 2^{pq} + 1 = (2^q)^p + 1$

$$= (2^q)^p - (-1)^p = \underbrace{(2^q - (-1))}_{A} \sum_{i=0}^{p-1} (-1)^{p-1-i} (2^q)^i$$

donc 2^{k+1} n'est pas premier car divisible par

$$A = 2^q + 1 > 1.$$

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$

b) on calcul F_5 : $\boxed{2^{2^5} + 1 = 641 \times 6700417}$

b) Soit $(n, a) \in \mathbb{N}^2$ $n > a$ montrons $F_n \wedge F_a = 1$

$$F_n - 2 = 2^{2^n} = \left(2^{2^a}\right)^{2^{n-a}}$$

$$= (F_a - 1)^{2^{n-a}}$$

$$\equiv (-1)^{2^{n-a}} \quad [F_a] \quad \text{Passage au modulo}$$

donc $F_n - 2 = 1 \; [F_a]$

d'où $F_a \mid F_n - 2$ donc $F_a \wedge F_n \mid F_n - 2$

pgcd

or $F_a \wedge F_n \mid F_n$

donc $F_a \wedge F_n \mid 2$

et F_a et F_n sont impairs donc $F_n \wedge F_a = 1$

c) notons p_n facteur premier de décomp de F_n, $n \in \mathbb{N}$.

d'après q. préc.,

Permet de dire qu'il y a une infinité de nombres premiers car $\forall n \in \mathbb{N}$ il existe au moins 1 diviseur premier, $\exists$ au moins une infinité

Ex 2 – Théorème d'Euler. Soit $n \in \mathbb{N}^*$

$\forall \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^* \quad \bar{x}^{\varphi(n)} = \bar{1} \qquad x^{\varphi(n)} = 1\ (n)$

Petit th de Fermat, p premier alors

$\forall \bar{x} \in (\mathbb{Z}/p\mathbb{Z})^* \quad \bar{x}^{p-1} = \bar{1}$, si p premier et si x est l'entier naturel et si $p \wedge x = 1$

alors $p \mid x^{p-1} - 1$

1°/ ~~$(p-1)(q-1) = \varphi(pq)$~~ indicatrice d'Euler $p \wedge q = 1$

$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$a \in \mathbb{Z}$ non divisible par p et q et $p \wedge q = 1$

donc $a \wedge p = 1$, $a \wedge q = 1$ $\Rightarrow a \wedge pq = 1$

d'après Euler $a^{(p-1)(q-1)} \equiv 1\ (pq)$.

2°/ Déterminer l'inverse de e modulo $(p-1)(q-1)$

on se place dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$

$e \wedge (p-1)(q-1) = 1$ donc $\bar{e}$ est inversible dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ (dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$)

$\exists\, d \in \mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ tq $\bar{e}d = 1\ (p-1)(q-1)$

~~Soit d la réciproque de~~ par choix de réciprocité des exposants entre 1 et $(p-1)(q-1)$

3°/

1) Si a n'est pas un multiple de p, un multiple de q.

$a^{(p-1)(q-1)} \equiv 1\ (pq)$ et $ed \equiv 1\ [(p-1)(q-1)]$

$\exists\, k \in \mathbb{Z} \quad ed = 1 + (p-1)(q-1)k$

Exo 1) $\Omega = \{1, \dots n\}$ $A = \mathcal{P}(\Omega)$

P probabilité uniforme chaque sujet est affecté d'une probabilité $\frac{1}{n}$.

2) P uniforme $P(A) = \dfrac{\text{Card}(A)}{\text{Card}\,\Omega} = \dfrac{\varphi(n)}{n}$

3) $P(A_i) = \dfrac{\text{Card}\,A_i}{\text{Card}\,\Omega}$ $\quad A_i = \left\{ k p_i \;/\; 1 \le k \le \dfrac{n}{p_i} \right\}$

donc $\text{Card}\,A_i = \dfrac{n}{p_i}$

$$P(A_i) = \frac{1}{p_i}$$

4) $i_1, \dots i_j$ éléments de $[\![1, \ell]\!]$

$A_{i_1} \cap \dots \cap A_{i_j}$ est réalisé ssi ω obtenu est divisible par chacun $p_{i_1} \dots p_{i_j}$ or $p_{i_k} \wedge p_{i_\ell} = 1$

ssi obtenu est divisible par produit (Gauss)

$$\tilde{A} = A_{i_1} \cap \dots A_{i_j} = \left\{ k\, p_{i_1} \dots p_{i_j} \;/\; 1 \le k \le \frac{n}{p_{i_1} \dots p_{i_j}} \right\}$$

$$\text{Card}(\tilde{A}) = \frac{n}{p_{i_1} \dots p_{i_j}}$$

donc $P(\tilde{A}) = \dfrac{1}{p_{i_1} \dots p_{i_j}} = P(A_{i_1}) \dots P(A_{i_j})$

Evts indép

5) Le nb obtenu est premier avec n ssi il n'est divisible par aucun p_i

donc $A = \bigcap_{i=1}^{\ell} \overline{A_i}$. Indép des $A_i \Rightarrow$ indép $\overline{A_i}$

$$P(A) = \prod_{i=1}^{\ell} P(\overline{A_i}) = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)$$

et $P(A) = \dfrac{\varphi(n)}{n}$ - résultat

$a^{ed} = a^{1+k(p-1)(q-1)} = a\, a^{k(p-1)(q-1)} = a\, 1^k = a \ (pq)$ Fermat

S: ~~si multiple de p et q alors pq | a~~

$p \mid a$ alors $p \mid a^{ed}$

donc $a^{ed} = a \ (p) = a \ (p)$

idem pour q.

B] a multiple de p ou q

i) a multiple de p et q alors $pq \mid a$

$pq \mid a^{ed}$

donc $pq \mid a^{ed} - a$

et $a^{ed} = a \ (pq)$

ii) a multiple de p mais pas de q.

($p \mid a$ et donc $p \mid a^{ed}$

$p \mid a^{ed} - a$

Par petit de Fermat. $a^{q-1} = 1 \ (q)$

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

et $a^{ed} = a^{1+(p-1)(q-1)k} = a \ (q)$

donc $a^{ed} - a$ divisible par q.

et ici il est divisible par p.

et $p \wedge q = 1$ $a^{ed} = a \ (pq)$

$e = 7$ $7 \wedge 20 = 1$ calcul de d par Bezout $d = 3$

$(33, 3)$ CC pour

$(33, 7)$ — publique

$m = 9 \Rightarrow m^e = 9^7 = 4782969 \equiv 15 \ [33]$

pour $15^3 = 3375 = 5 \ [33]$