Leçon 121 : Nombres premiers. Applications.

1 L'ensemble des nombres premiers

1.1 Introduction aux nombres premiers

Définition 1 (ROM 303)**.** On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple 2 (No ref)**.** $2, 3, 5, 7$ sont des nombres premiers. Cependant $4 = 2 \times 2$ et $6 = 2 \times 3$ ne sont pas premiers.

Théorème 3 (ROM 303)**.** [Euclide] Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Théorème 4 (ROM 305)**.** [lemme d'Eulcide] Soit $(n_k)_{1 \leq k \leq r}$ une suite de $r \geq 2$ entiers naturels non nuls. Un nombre premier p divise le produit $\prod_{k=1}^{r} n_k$ si et seulement si il divise l'un des n_k.

1.2 Décomposition en produit de facteurs premiers

Théorème 5 (ROM 306)**.** [fondamental de l'arithmétique] Tout entier $n \geq 2$ se décompose de manière unique sous la forme :

$$n = q_1^{\alpha_1} ... q_r^{\alpha_r}$$

où les q_k sont des nombres premiers tels que $2 \geq q_1 < q_2 < ... < q_r$ et les α_k sont des entiers naturels non nuls.

Définition 6 (ROM 306)**.** On appelle la valuation $p-$adique de n, et on note $v_n(p)$, l'exposant de p dans la décomposition en facteurs premiers, avec $v_n(p) = 0$ si p n'apparait dans cette décomposition.

Notation 7 (ROM 306, TL1 87)**.** Cette notation est complété en posant $v_p(1)$ pour tout $p \in \mathcal{P}$.

Théorème 8 (TL1 87, ROM 307)**.** Soient x, y deux entiers strictement positifs. x divise y si et seulement si $v_p(x) \leq v_p(y)$ pour tout nombre premier p.

Théorème 9 (ROM 307)**.** Soient $n \geq 2$ et $m \geq 2$ deux entiers de décomposition en facteurs premiers : $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, $m = \prod_{k=1}^{\beta_k}$ où les q_k sont des nombres premiers deux à deux distincts et les α_k, β_k des entiers naturels. On a alors :
$n \wedge m = \prod_{k=1}^{r} q_k^{\min(\alpha_k, \beta_k)}$ et $n \vee m = \prod_{k=1}^{r} q_k^{\max(\alpha_k, \beta_k)}$

Méthode 10 (No ref)**.** Pour trouver le pcgd ou le ppcm de deux nombres, on peut donc se ramener à étudier leur décomposition en produit de facteurs premiers.

Exemple 11 (No ref)**.** Considérons 60 et 252. On a les décompositions en facteurs premiers : $60 = 2^2 \times 3 \times 5$ et $252 = 2^2 \times 3^2 \times 7$. Leur pgcd est donc $2^2 \times 3 = 12$ et leur ppcm $2^2 \times 3^2 \times 5 \times 7 = 252$.

1.3 Répartition des nombres premiers

On a vu qu'on a des résultats pratique avec les nombres premiers maintenant les questions qui se posent vont être, comment trouver de tels nombres ?

Proposition 12 (TL1 84)**.** Soit $n > 1$. Si n n'est pas premier, il possède un facteur premier p tel que $p^2 \leq n$.

Méthode 13 (No ref)**.** Pour vérifier qu'un nombre est premier, il suffira donc de vérifier qu'il n'est divisible par aucun entier entre 2 et $Ent(\sqrt{n})$

Ceci nous donne les nombres premiers qui divise un certain entier n. Maintenant on va vouloir chercher tous les nombres premiers plus petit que n.

Algorithme 14 (TL1 84)**.** [Crible d'Ératosthène] Soit $n \geq 1$. Dans la liste des entiers de 2 à n on supprime tous les mutliples de 2, puis tous les multiple de 3, etc. Après avoir supprimé tous les multiples d'un certain entier, le plus petit des entiers qui restent dans la liste, s'il y en a, est premier. On obtient ainsi successivement tous les nombres premiers entre 2 et n. (cf annexe)

Proposition 15 (ROM 326, cf selon demo simple ou pas)**.** n est premier si et seulement si $\binom{n}{k} \equiv 0 \pmod{n}$ pour tout $1 \leq k \leq n-1$

Théorème 16 (ROM 284)**.** [Fermat] Soit $p \in \mathcal{P}$. Pour tout $a \in Z$, $a^p \equiv a \pmod{p}$.

Méthode 17 (No ref)**.** Ce théorème nous donne un test de non primalité

Exemple 18 (No ref)**.** $2^4 = 16 \equiv 0 \pmod{4}$ donc 4 n'est pas premier.

Contre-exemple 19 (ROM 329)**.** Attention, la réciproque est fausse, cela n'est donc pas suffisant pour dire qu'un nombre est premier : $561 = 3 \times 11 \times 17$. Or 560 est divisible par 2, 10 et 16 doncc pour tout $a \in \mathbb{Z}$, $a^{560} \equiv 1 \pmod{p_k}$, pour tout $p_k \in \{3, 11, 17\}$. On en déduit que a^{560} est premier avec $3 \times 11 \times 17$ pour tout a et on a donc $a^{560} \equiv 1 \pmod{560}$ pour tout $a \in \mathbb{Z}$.
Les nombres vérifiant cette propriété sans être premiers sont appelés les nombre de Carmichaël.

Théorème 20 (TL1 85)**.** [d'Euclide] L'ensemble $\mathcal{P}$ des nombres premiers est infini.

2 Nombres premiers remarquables

2.1 Nombres de Mersenne

Proposition 21 (ROM 337, TL1 84)**.** Soient $a \geq 2$ et $n \geq 2$ deux nombres entiers. Considérons $p = a^n - 1$. Si p est premier, alors $a = 2$ et n est premier.

Définition 22 (TL1 84, ROM 304)**.** De tels nombres $2^n - 1$ où n est premier sont appelé nombres de Mersenne.

Exemple 23 (No ref)**.** $2^2 - 1 = 3$ et $2^3 - 1 = 7$ sont premiers.

Contre-exemple 24 (No ref)**.** $2^4 - 1 = 15 = 3 \times 5$ n'est pas premier. Ceci montre que la réciproque est fausse.

2.2 Nombres de Fermat

Proposition 25 (ROM 340)**.** Soit $a \geq 2$ et $m \geq 1$ deux entier. On considère $p = a^m + 1$. Si p est premier, a est pair et il existe $n \geq 0$ tel que $m = 2^n$.

Définition 26 (ROM 340)**.** De tels nombres avec $q = 1$, c'est-à-dire des nombres de la forme $2^{2n} + 1$ avec $q \geq 1$ et $n \in \mathbb{N}$, sont appelés nombres de Fermat.

Exemple 27 (TL1 85)**.** $2^{2^1} + 1 = 5$ est premier.

Contre-exemple 28 (TL1 85)**.** $2^{2^5} + 1$ n'est pas premier. La réciproque de la proposition est donc fausse.

2.3 Nombres de Sophie Germain

Théorème 29 (TL1 138)**.** [dernier théorème de Fermat, admis] Pour des entiers $n \leq 3$ et $xyz \neq 0$, l'égalité $x^n + y^n = z^n$ est impossible.

Exemple 30 (No ref)**.** Pour $n = 2$, $(x, y, z) = (3, 4, 5)$ est une solution de cette équation.

Définition 31 (ORAUX XENS Al1)**.** On appelle nombre de Sophie Germain un nombre premier p tel que p est impair et $q = 2p + 1$ est premier

Théorème 32 (ORAUX XENS Al1)**.** [Théorème de Sophie Germain][DEV 2] Soit p un nombre premier de Sophie Germain. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tels que $xyz \not\equiv 0$ $[p]$ et $x^p + y^p + z^p = 0$

3 Applications

3.1 En probabilités

Proposition 33 (..)**.** [DEV1] Notons $(p_n)_{n\leq 1}$ la suite des nombres premiers dans l'ordre croissant ($p_1 = 2, p_2 = 3, ..$). On a

$$\sum_{k=1}^{+\infty} \frac{1}{p_n} = +\infty$$

Lemme 34 (BL 93)**.** [DEV1] Soit $(A_n)_n$ une suite d'évènements.

1. Si $\sum\limits_{n\in\mathbb{N}} \mathbb{P}(A_n) < +\infty$ alors $\mathbb{P}(A_n i.s.) = 0$
2. Si $(A_n)_n$ est indépendante, alors :

$$\sum_{n\in\mathbb{N}} \mathbb{P}(A_n) = +\infty \implies \mathbb{P}(A_n i.s.) = 1$$

Application 35 (no ref)**.** [DEV1] Il n'existe pas de mesure de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que $\mathbb{P}(\text{multiple de n}) = \frac{1}{n}$, pour tout $n \in \mathbb{N}^*$

3.2 Irréductibilité des polynômes

Définition 36 (ROM 382)**.** Le contenu d'un polynôme $P(X) = \sum\limits_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ est l'entier $c(P) = pgcd(a_0, .., a_n)$.
Si $c(P) = 1$, on dit que P est primitif

Lemme 37 (GOU 62)**.** Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. Si p divise tous les coefficients de PQ, alors p divise tous les coefficients de P ou tous ceux de Q.

Lemme 38 (GOU 62)**.** Si $P, Q \in \mathbb{Z}[X]$ alors $c(PQ) = c(P)c(Q)$.

Lemme 39 (GOU 62)**.** Si $\phi \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.

Théorème 40 (GOU 62)**.** Soit $P = a_n X^n + .. + a_1 X + a_n \in \mathbb{Z}[X]$ et p un nombre premier. Si on a :

1. p ne divise pas a_n
2. p divide a_i, pour tout $1 \leq i \leq n - 1$
3. p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 41 (GOU 62)**.** Si p est premier, $\phi(X) = X^{p-1} + ... + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

3.3 Aux corps finis

Dans cette sous-partie, A représente un anneau unitaire et intègre.

Proposition et définition 42 (ROM 415)**.** $\varphi : n \in \mathbb{Z} \mapsto n \cdot 1 \in A$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Il existe un unique entier $p \in \mathbb{N}$ tel que $ker(\varphi) = p\mathbb{Z}$.
On dit que p est la caractéristique de A.

Proposition 43 (ROM 415)**.** La caractéristique d'un anneau unitaire intègre est 0 ou un nombre premier.

Corollaire 44 (No ref)**.** En particulier, la caractéristique d'un corps est soit nulle soit un nombre premier.

Théorème 45 (ROM 416)**.** Si $\mathbb{K}$ est un corps fini, il est alors de cardinal p^n, où $p \geq 2$ est un nombre premier (la caractéristique de $\mathbb{K}$) et n un entier naturel non nul.
Dans ce cas, tout sous-corps de $\mathbb{K}$ est de cardinal p où d est un diviseur de n.
Réciproquement, pour tout diviseur d de n, il existe un unique sous-corps de $\mathbb{K}$ de cardinal p à savoir le corps $\mathbb{F} = \{x \in \mathbb{F}_p | ^{x^p} = x\}$