Nombres premiers. Applications.

Mohamed NASSIRI

L'idée de départ est de trouver une "décomposition atomique" des nombres entiers. Ces "atomes" sont les nombres premiers. Même si leur définition paraît simple et que par le théorème d'Euclide on sait qu'il existe une infinité de nombres premiers, il subsiste néanmoins plusieurs problèmes encore non résolus sur les nombres premiers et leur répartition. Fort heureusement, il existe quand même des critères de primalité et plusieurs résultats intéressants, et la notion de "nombres premiers entre eux" va enrichir les résultats.

L'un des premiers gros théorème sur lequel on tombe est le *Théorème fondamental de l'arithmétique* qui nous dit que tout nombre naturel $n > 1$ peut s'écrire comme un produit de nombres premiers (et cette représentation est unique, à part l'ordre dans lequel les facteurs premiers sont disposés). Même si ce résultat peut nous paraître évident, il n'en est rien ... Illustrons notre propos en considérant l'ensemble $E = \{2n \mid n \in \mathbb{N}\}$. Dans E, 12 est composé ($12 = 6 \times 2$) tandis que 10 est premier (10 ne s'écrit pas comme le produit de deux nombres de E). Les nombres premiers de E sont donc $2, 6, 10, 14, 18, 22, 26, 30, 34...$ Par ailleurs, si on considère 60, on remarque que $60 = 2 \times 30 = 6 \times 10$ et donc la décomposition en nombres premiers dans cet ensemble n'est pas unique !

S'il y a quelque chose qu'il faut savoir sur les nombres premiers, c'est que l'on a aucune formule explicite (de type polynomiale) pour tous les atteindre. D'ailleurs, on peut démontrer que c'est impossible. En revanche, *le théorème de Dirichlet* assure qu'il en existe une infinité sous une forme polynomiale de degré 1.

Le célèbre *théorème d'Euler* nous conduira à un autre célèbre théorème : le *théorème des restes chinois*. Il permet de résoudre des systèmes de congruences de la forme :

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_r \pmod{m_r} \end{cases}$$

Une brève excursion chez les nombres de Mersenne et de Fermat nous donnera quelques résultats de primalité supplémentaires :

Nombre de Mersenne : $M_n = 2^n - 1$, où $n \in \mathbb{N}$
Si $(2^m - 1)$ est un nombre premier, alors m est aussi un nombre premier.

Nombre de Fermat : $\mathrm{Fer}_n = 2^{2^n} + 1$, où $n \in \mathbb{N}$
Si $2^m + 1$ est un nombre premier, alors m est une puissance de 2.

Les applications concernant les nombres premiers sont variées. Les corps finis pour commencer : quand p est premier, l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, et on a plusieurs résultats intéressants. Par exemple, on a deux résultats sur l'irréductibilité des polynômes : le critère d'Eisenstein et le critère de réduction. Mais également, l'étude des carrés de $\mathbb{Z}/p\mathbb{Z}$ va nous conduire au célèbre "théorème des deux carrés".

Références

[KM] Introduction à la théorie des nombres, Jean-Marie De Koninck et Armel Mercier
[GOZ] Théorie de Galois, Ivan Gozard
[TOU] Arithmétique, Chédly Touibi
[PER] Cours d'Algèbre, Daniel Perrin
[FGNag1] Algèbre 1 Oraux X-ENS, Serge Francinou, Hervé Gianella et Serge Nicolas
[ML3ag] Mathématiques Algèbre L3, Aviva Szpirglas

Développements

Théorème de Dirichlet (version faible)
Théorème des deux carrés
Existence et unicité des corps finis
Critère d'Eisenstein

1 Définitions et premières propriétés

1.1 Nombres premiers et nombres premiers entre eux [KM] p.11-12,21-22

Définition 1 *Un entier $p > 1$ est appelé un nombre premier si ses seuls diviseurs sont 1 et p. Un entier plus grand que 1 qui n'est pas premier est dit composé.*

Exemple 2 *Liste des nombres premiers $p < 50$: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.*

Définition 3 *On dit que les entiers $a_1, ...a_n$ sont (relativement) premiers entre eux si $(a_1, ...a_n) := \text{pgcd}(a_1, ...a_n) = 1$.*

Théorème 4 *Soit $a, b \in \mathbb{Z}$ tels $ab \neq 0$. Alors $(a, b) = 1 \Leftrightarrow$ il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$*

Théorème 5 *Soit $a, b, m \in \mathbb{Z}\backslash\{0\}$. Alors*

$$(a, m) = (b, m) = 1 \Leftrightarrow (ab, m) = 1$$

Corollaire 6 *Si $(a, b) = 1$, alors $(a^n, b^k) = 1$ $\forall n, k \in \mathbb{N}$.*

Théorème 7 *Lemme de Gauss : Si $a \mid bc$ et $(a, b) = 1$, alors $a|c$.*

Corollaire 8 *Si $b \mid a$ et $c \mid a$, où $(b, c) = 1$, alors $bc \mid a$.*

Corollaire 9 *Si $(a, b) = 1$, alors $(ac, b) = (c, b)$.*

Théorème 10 *Lemme d'Euclide : Si p est premier et $p \mid ab$ alors $p \mid a$ ou $p \mid b$.*

Corollaire 11 *Si p est premier et $p \mid a_1 a_2 ... a_r$ alors il existe un entier k, avec $1 \leq k \leq r$ tel que $p \mid a_k$.*

Corollaire 12 *Si $p, q_1, ..., q_r$ sont des nombres premiers et si $p \mid q_1 ... q_r$, alors $p = q_k$ pour un certain k tel que $1 \leq k \leq r$.*

1.2 Factorisation [KM] p.22 → 25

Théorème 13 *Théorème fondamental de l'arithmétique*
Tout nombre naturel $n > 1$ peut s'écrire comme un produit de nombres premiers, et cette représentation est unique, à part l'ordre dans lequel les facteurs premiers sont disposés.

Corollaire 14 *Tout nombre naturel $n > 1$ peut s'écrire de façon unique sous la forme*

$$n = q_1^{a_1} q_2^{a_2} ... q_r^{a_r}$$

où les q_i sont des nombres premiers distincts et où les a_i sont des entiers positifs.

Exemple 15 $60 = 2^2.3.5$

Remarque 16 *Pour comparer deux nombres, on fait souvent apparaître des puissances nulles :* $10 = 2.3^0.5$, $6 = 2.3.5^0$ ...

Théorème 17 *Soit $n = \prod_{i=1}^r q_i^{a_i}$, avec $a_i > 0$ pour chaque i et soit $d > 0$.*
Alors $d \mid n \Leftrightarrow d = \prod_{i=1}^r q_i^{b_i}$ pour certains entiers non négatifs $b_i \leq a_i$, $i = 1, ..., r$.

Théorème 18 *Si $a = \prod_{i=1}^r q_i^{\alpha_i}$ et $b = \prod_{i=1}^r q_i^{\beta_i}$, avec $\alpha_i > 0$ et $\beta_i > 0$ pour chaque i, sont les représentations canoniques de a et b, alors :*

$$\text{pgcd}(a, b) = \prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i)} \quad \text{et}$$

$$\text{ppcm}(a, b) = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i)}$$

1.3 Critères de primalité [KM] p.42 → 47

Proposition 19 *Le crible d'Eratosthène :*
Un entier naturel n strictement supérieur à 1 qui n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ est premier. **[KM] p.25-26**

Théorème 20 *La fonction d'Euler Φ est définie par :*

$$\Phi(m) = \#\{n \leq m \mid (n, m) = 1\}$$

Exemple 21 $\Phi(6) = 2$, $\Phi(12) = 4$ *et* $\Phi(p) = p - 1$ *pour tout nombre premier p.*

Théorème 22 *Théorème d'Euler*
Soit $(a, m) = 1$, alors $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Théorème 23 *Petit théorème de Fermat*
Soit p un nombre premier et soit a un entier positif tel que $p \nmid a$. Alors $a^{p-1} \equiv 1 \pmod{p}$. De plus, $\forall a \in \mathbb{N}$, on a $a^p \equiv a \pmod{p}$.

Remarque 24 *Le dernier chiffre dans la représentation décimale de 3^{945} est 3, et 3 et 4 sont les deux derniers.*

Théorème 25 *Si $(a, m) = 1$, alors la congruence $a \equiv b \pmod{m}$ possède une solution x_0 et toutes les autres sont données par :*

$$x = x_0 + km, \qquad k \in \mathbb{Z}$$

Théorème 26 *Théorème de Wilson :*
Soit $m \in \mathbb{N}^*$. Alors

$$m \text{ est premier} \Leftrightarrow (m-1)! \equiv -1 \pmod{m}$$

Exemple 27 $100!+1$ *n'est pas premier car* $101 \mid 100!+1$

Théorème 28 *Théorème des restes chinois :*
Soient $m_1, ..., m_r$ *des nombres naturels relativement premiers deux à deux et* $a_1, ..., a_r$ *des entiers quelconques. Alors le système de congruences :*

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_r \pmod{m_r} \end{cases}$$

possède une solution. De plus, toutes les solutions sont congrues modulo $m_1...m_r$

Exemple 29 *Le plus petit entier positif* x *tel que :*

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

est $x_0 = 256 \equiv 53 \pmod{105}$

2 Répartition des nombres premiers

2.1 Répartition [KM] p.24 → 32

Exemple 30 233 *n'est divisible par* 2, *ni par* 3,5, 7, 11 *et* 13 *(et inutile de vérifier pour les nombres supérieurs* 17 *car* $17^2 = 289 > 233$*). Ainsi* 233 *est premier.*

Théorème 31 *Théorème d'Euclide :*
Il existe une infinité de nombres premiers.

Théorème 32 *Soit* f *un polynôme non constant à coefficients entiers. Alors* $f(n)$ *ne peut représenter un nombre premier pour tout* $n \in \mathbb{N}$.

Exemple 33 $f(m) = m^2 + m + 41$. $\forall m \in [\![0; 39]\!]$, $f(m)$ *est premier mais* $f(40) = 41^2$ *et* $f(41) = 41 \times 43$

Théorème 34 *Théorème de Dirichlet (version faible) :* ♠
a) $\Phi_n(X)$ *désigne le* n*-ième polynôme cyclotomique. Si un nombre premier* p *divise* $\Phi_n(a)$ *pour un certain* $a \in \mathbb{N}$, *mais aucun des* $\Phi_d(a)$ *où* $d \mid n$, $d < n$, *alors* $p \equiv 1 \pmod n$
b) Il existe une infinité de nombres premiers de la forme $1 + \lambda n$, $\lambda \in \mathbb{N}^*$. **[GOZ] p.84**

Définition 35 *La fonction*

$$\pi(x) := \sum_{p \leq x} 1$$

compte le nombre de nombres premiers $p \leq x$.

Théorème 36 $\lim\limits_{x \to +\infty} \pi(x) = +\infty$ *et* $\pi(x) \sim \frac{x}{\log(x)}$

Théorème 37 (admis) *Inégalités de Tchebycheff :*
Pour chaque $x \geq 2$, *on a :*

$$\frac{\log(2)}{4} \frac{x}{\log(x)} < \pi(x) < 9\log(2) \frac{x}{\log(x)}$$

Lemme 38 *Si* $n \geq 1$, *alors* $\prod_{p \leq n} p < 4^n$

Théorème 39 (admis) *Postulat de Bertrand :*
$\forall n \in \mathbb{N}$, $\exists p$ *premier tel que* $n < p < 2n$

Lemme 40 $\forall k \geq 1$, *on a*

$$\log(k) < \sum_{n=1}^{k} \frac{1}{n} \leq \log(k) + 1$$

Remarque 41 *Un raffinement nous donne le développement asymptotique de la série harmonique ...*

Théorème 42 $\forall x \geq 3$, $\exists c_1, c_2 > 0$ *telles que :*

$$c_1 \text{loglog}(x) < \sum_{p \leq x} \frac{1}{p} < c_2 \text{loglog}(x)$$

2.2 Quelques conjectures [KM] p.217-218

Conjecture 43 *Existe-t-il une infinité de nombres premiers de la forme* $n^2 + 1$, $n \in \mathbb{N}$ *?*

Conjecture 44 *Existe-t-il une infinité de nombres premiers de la forme* $n! + 1$, $n \in \mathbb{N}$ *?*

Conjecture 45 *Existe-t-il une infinité de nombres premiers jumeaux, c'est à dire des nombres premiers* p_n *et* p_{n+1} *tels que* $p_{n+1} - p_n = 2$ *? Cousins ? Sexys ?*

Conjecture 46 *Soit* $2 \leq x, y \in \mathbb{N}$, $\pi(x + y) \leq \pi(x) + \pi(y)$ *?*

3 Nombres de Mersenne et de Fermat [TOU] p.57-62

3.1 Nombres de Mersenne

Définition 47 *Un entier de la forme* $M_n = 2^n - 1$, *où* $n \in \mathbb{N}$, *est appelé nombre de Mersenne.*

Théorème 48 *Si* $(2^m - 1)$ *est un nombre premier, alors* m *est aussi un nombre premier.*

Proposition 49 *Soient* M_p *et* M_q *deux nombres de Mersenne avec* $p \neq q$, *alors* $\text{PGCD}(M_p, M_q) = M_{\text{PGCD}(p,q)}$

3.2 Nombres de Fermat

Définition 50 *On appelle nombre de Fermat nn entier de la forme* $\text{Fer}_n = 2^{2^n} + 1$, *où* $n \in \mathbb{N}$.

Théorème 51 *Si* $2^m + 1$ *est un nombre premier, alors* m *est une puissance de 2.*

Proposition 52 $\forall m, n \in \mathbb{N}^*$, $m \neq n$, $\text{PGCD}(\text{Fer}_n, \text{Fer}_m) = 1$

4 Applications

4.1 Corps finis

Proposition 53 *Soit* $p \in \mathbb{N}$, $p \geq 2$. *Les asserstions suivantes sont équivalentes :*
(i) p *est un nombre premier*
(ii) $\mathbb{Z}/p\mathbb{Z}$ *est un anneau intègre*
(iii) $\mathbb{Z}/p\mathbb{Z}$ *est un corps* **[GOZ] p.3**

Remarque 54 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ *et c'est un corps fini,* $|\mathbb{F}_p| = p$.

Théorème 55 *Existence et unicité des corps finis* ♠
Soient p *un nombre premier,* $n \in \mathbb{N}^*$. *On note* $q = p^n$.
(1) Il existe un unique corps fini à q *éléments, à isomorphisme près. Il est le corps de décomposition sur* $\mathbb{F}_p$ *du polynôme* $X^q - X$.
(2) $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, *où* π *est un polynôme irréductible quelconque de degré* n *sur* $\mathbb{F}_p$.
(3) Si π *est un polynôme irréductible de degré* n *sur* $\mathbb{F}_p$, *alors* $\pi(X) \mid X^q - X$ *dans* $\mathbb{F}_p[X]$, *donc scindé sur* $\mathbb{F}_q$. *Ainsi son corps de rupture* $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ *est aussi son corps de décomposition.* **[GOZ] p.85,87-88**

4.2 ♠ Théorème des deux carrés ♠ [PER] p.56 → 58, 74-75

Définition 56 *On pose* $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2 = n\}$

Lemme 57 $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{N}\}$ *est un anneau euclidien* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Lemme 58

$$p \in \Sigma \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$
$$\Leftrightarrow -1 \in \mathbb{F}_p^{*2}$$

Théorème 59 $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod 4$

4.3 Irréductibilité des polynômes

Théorème 60 *Critère d'Eisenstein* ♠
Soit $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ *et* p *un nombre premier. On suppose que :*

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad \text{, et} \quad (iii)\ p^2 \nmid a_0$$

Alors P *est irréductible dans* $\mathbb{Q}[X]$.
Si $c(P) = 1$, *alors* P *est irréductible dans* $\mathbb{Z}[X]$. **[FGNag1] p.145**

Exemple 61 *1)* $\forall p$ *premier,* $X^n - p$ *est irréductible dans* $\mathbb{Q}[X]$ *et* $\mathbb{Z}[X]$.
2) $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$ *st irréductible dans* $\mathbb{Z}[X]$. **[ML3ag] p.549**

Théorème 62 *Critère de réduction modulo p :*
Soit p *un nombre premier. Soit* $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ *et* $\overline{P} = \overline{a_n} X^n + ... + \overline{a_1} X + \overline{a_0}$, *où* $\overline{a_i}$ *est la classe des* a_i *dans* $\mathbb{Z}/p\mathbb{Z}$
Alors si $\overline{P}$ *est irréductible sur* $\mathbb{F}_p$, P *est irréductible sur* $\mathbb{Z}$.
Si $c(P) = 1$, *alors* P *est irréductible dans* $\mathbb{Z}[X]$. **[ML3ag] p.550**

Exemple 63 $P(X) = X^3 + 462X^2 + 2433X - 67691$ *est irréductible dans* $\mathbb{Z}[X]$ **[PER] p.77**

Théorème 64 *Soit* $P \in k[X]$ *un polynôme irréductible de degré* n *et soit* K *une extension de* k *de degré* m *avec* $(m, n) = 1$.
Alors P *est encore irréductible sur* K. **[PER] p.79**

Questions

Exercice : Crible d'Eratosthène et théorème d'Euclide
1) *Crible d'Eratosthène :* Montrer qu'un entier naturel n strictement supérieur à 1 qui n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ est premier.
2) *Théorème d'Euclide :* Montrer qu'il existe une infinité de nombres premiers.

Solution : 1) *A priori*, le crible "naïf" (et évident) d'Eratosthène nous dit qu'un entier naturel n strictement supérieur à 1 qui n'est divisible par aucun nombre premier inférieur ou égal à n est premier. Ici, on aimerait montrer que l'on a pas besoin de vérifier pour des diviseurs premiers inférieur ou égal à n mais inférieur ou égal à $\sqrt{n}$.
En effet, supposons que n est composé et que tous les nombres premiers p qui divisent n vérifient

$$\sqrt{n} \leq p \leq n \qquad (\dagger)$$

Par suite, si un certain nombre premier p_0 divise n et vérifie (†), on peut donc écrire $n = p_0 n_0$ pour un certain entier $n_0 > 1$. Or, on a $n_0 \mid n$ et

$$n_0 = \frac{n}{p_0} < \frac{n}{\sqrt{n}} = \sqrt{n}$$

Par conséquent, on a un diviseur de n qui possède au moins un facteur premier inférieur à $\sqrt{n}$. Absurde.

2) Cette démonstration est très classique et élémentaire !
Supposons le contraire (*i.e.*) qu'il existe un nombre fini de nombres premiers, que nous noterons p_1, p_2,..., p_k. Considérons le nombre

$$N = p_1 p_2 ... p_k + 1$$

Si N est premier, alors on a trouvé un nombre premier plus grand que p_k, et on a donc une contradiction.
Si N est composé, alors N est divisible un nombre premier (*i.e.*) qu'il existe $i \in \{1, ..., k\}$ tel que $p_i \mid N$, mais alors on aurait $p_i \mid 1$. Absurde.

Remarque : Attention, les entiers

$$M_k = p_1 p_2 ... p_k + 1$$

ne sont pas tous premiers. En effet, $M_6 = 30031 = 59.509$. De nos jours, on ne sait pas si la suite $(M_k)_{k \in \mathbb{N}}$ contient une infinité de nombres premiers ...

Exercice : Théorème fondamental de l'arithmétique
1) Montrer que tout nombre naturel $n > 1$ peut s'écrire comme un produit de nombres premiers, et cette représentation est unique, à part l'ordre dans lequel les facteurs premiers sont disposés.
2) Soient $a = \prod_{i=1}^{r} q_i^{\alpha_i}$ et $b = \prod_{i=1}^{r} q_i^{\beta_i}$, avec $\alpha_i > 0$ et $\beta_i > 0$ pour chaque i, les représentations canoniques de a et b. Montrer que :

$$\text{pgcd}(a,b) = \prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad \text{ppcm}(a,b) = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i)}$$

Solution : 1) Si n est premier, alors il n'y a rien à démontrer.
Supposons donc que n soit composé et considérons l'ensemble.

$$D = \{d \mid d \mid n \text{ et } 1 < d < n\}$$

Alors, $D \subset \mathbb{N}$ et comme n est composé, $D \neq \varnothing$. D'après le principe du bon ordre, D possède un plus petit élément p_1 qui est premier (par minimalité de p_1). On peut donc écrire

$$n = p_1 n_1$$

Si n_1 est premier, c'est terminé. Sinon, on répète le même argument. On en déduit l'existence d'un nombre premier p_2 et d'un nombre $n_2 < n_1$ tels que $n = p_1 p_2 n_2$. Ainsi, à la k-ième étape, on aura

$$n = p_1 p_2 .... p_k n_k \quad \text{avec} \quad n_1 > n_2 > ... > n_k > 1$$

Puisque les n_i sont des entiers, le processus a une fin et on arrive à une k-ième étape où n_k est premier (*i.e.*) $n_k = p_{k+1}$. Par suite,

$$n = p_1 p_2 .... p_k p_{k+1}$$

Il nous reste donc à montrer l'unicité de cette décomposition. Supposons le contraire (*i.e.*) que l'on a

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_r$$

avec p_i et q_j des nombres premiers non nécessairement distincts.
On simplifie l'égalité en éliminant les nombres premiers qui apparaissent des deux côtés à la fois. On aura donc

$$p_{i_1} p_{i_2} ... p_{i_\alpha} = q_{j_1} q_{j_2} ... q_{j_\beta} \qquad (\dagger\dagger)$$

avec $\alpha \leq r$ et $\beta \leq s$. Ainsi, dans $(\dagger\dagger)$, tous les p_i sont différents des q_j. Mais ceci est impossible car on aurait $p_{i_1} \mid q_{j_1} q_{j_2} ... q_{j_\beta}$ et donc qu'il existe un entier ρ $(1 \leq \rho \leq \beta)$ tel que $p_{i_1} = q_{j_\rho}$ ce qui contredit le fait que tous les p_i sont différents des q_j.

2) Soit $d = \prod_{i=1}^{r} q_i^{c_i}$, où $c_i = \min(\alpha_i, \beta_i)$. Puisque $c_i \leq \alpha_i$ et $c_i \leq \beta_i$, alors $d \mid a$ et $d \mid b$ et ainsi d est un diviseur commun de a et b.
Supposons que $g \mid a$ et $g \mid b$, alors on a nécessairement $|g| = \prod_{i=1}^{r} q_i^{e_i}$, où $e_i \leq \alpha_i$ et $e_i \leq \beta_i$ pour tout i mais puisque c_i est le plus petit des nombres α_i et β_i, on a donc $e_i \leq c_i$ pour tout i et par suite on a $g \mid d$. Par conséquent,

$$\prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i)} = d = \text{pgcd}(a, b)$$

Pour obtenir, $\text{ppcm}(a, b) = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i)}$, il suffit de remarque que l'on a les deux relations suivantes :

$$\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \max(\alpha_i, \beta_i)$$
$$\text{pgcd}(a, b)\text{ppcm}(a, b) = ab$$

Exercice : Soit f un polynôme non constant à coefficients entiers. Alors $f(n)$ ne peut représenter un nombre premier pour tout $n \in \mathbb{N}$.

Solution : Ecrivons ce polynôme sous la forme

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + ... + a_1 n + a_0$$

avec $k \geq 1$, $a_i \in \mathbb{Z}$ et $a_k \neq 0$.
Supposons que $f(n)$ soit premier pour chaque valeur de $n \in \mathbb{N}$ et prenons $n_0 \in \mathbb{N}$ et posons $f(n_0) = p_0$ pour un certain nombre premier p_0. Par suite, pour tout $t \in \mathbb{N}$, on a

$$\begin{aligned} f(n_0 + tp_0) &= a_k (n_0 + tp_0)^k + ... + a_1 (n_0 + tp_0) + a_0 \\ &= a_k n_0^k + ... + a_1 n_0 + a_0 + p_0 g(t) \end{aligned}$$

où $g(t)$ est un polynôme à coefficients entiers. On peut encore réécrire la relation précédente comme suit

$$f(n_0 + tp_0) = f(n_0) + p_0 g(t) = p_0 + p_0 g(t) = p_0 (1 + g(t))$$

On a donc démontré que si $f(n_0) = p_0$, alors on a automatiquement $p_0 \mid f(n_0 + tp_0)$ pour chaque valeur entière de t. Par suite, $f(n_0 + tp_0)$ est soit un nombre composé pour chaque valeur entière de t ce qui est une contradiction (puisque $f(n)$ est supposé premier pour chaque valeur de $n \in \mathbb{N}$), soit on a

$f(n_0+tp_0) \in \{0, -p_0, p_0\}$. Mais ceci est également absurde car un polynôme non constant de degré $k \geq 1$ ne peut donner la même valeur plus de k fois. D'où le résultat.

Remarque : Pourtant on peu construire des polynômes convaincants au premier abord. Par exemple, $f(m) = m^2 + m + 41$ est premier pour tout $m \in [\![0; 39]\!]$, $f(m)$ mais $f(40) = 41^2$ et $f(41) = 41 \times 43$ ...

Exercice : Nombres de Mersenne et de Fermat
On rappelle que :
- Un entier de la forme $M_n = 2^n - 1$, où $n \in \mathbb{N}$, est appelé *nombre de Mersenne.*
- Un entier de la forme $\text{Fer}_n = 2^{2^n} + 1$, où $n \in \mathbb{N}$, est appelé *nombre de Fermat*

1)a) Montrer que si $(2^m - 1)$ est un nombre premier, alors m est aussi un nombre premier.
b) La réciproque est-elle vraie ?
2)a) Montrer que si $2^m + 1$ est un nombre premier, alors m est une puissance de 2.
b) La réciproque est-elle vraie ?

Solution : 1) Raisonnons par l'absurde. Supposons que l'entier m soit un nombre composé et posons

$$m = ab \quad \text{avec} \quad 1 < a < m \text{ et } 1 < b < m$$

On a donc

$$2^m - 1 = ((2^a)^b - 1) = (2^a - 1)((2^a)^{b-1} + ... + 1)$$

Cette égalité contredit le fait que $2^m - 1$ est premier (car $1 < 2^a - 1 < 2^m - 1$).

b) Non. Par exemple, 11 est premier alors que $2^{11} - 1 = 2047 = 23 \times 89$.

2) Soit q un diviseur premier impair de m, et posons $m = qr$. Alors, on a

$$2^m + 1 = ((2^r)^q + 1) = (2^r + 1)((2^r)^{q-1} - (2^r)^{q-2} + ... + 1)$$

Cette égalité montre que $2^m - 1$ n'est pas premier (car $1 < 2^r + 1 < 2^m + 1$). Par conséquent, m n'a aucun diviseur premier impair.

b) Encore une fois, non ! Par exemple, pour $m = 2^5$, on a

$$\text{Fer}_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$$