Nombres premiers

Théorème : Il existe une infinité de nombres premiers

Preuve : Supposons qu'il y ait un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_n$

Ainsi p_n est le plus grand nombre premier

Posons $x = (p_1 p_2 \ldots p_n) + 1$

Ce x (qui est ≥ 2) est divisible par au moins un nombre premier p

Ainsi p divise x et p doit appartenir à l'ensemble composé de tous les premiers $\{p_1, \ldots, p_n\}$

Or si p divise x et divise $p_1 \ldots p_n$, alors ce p doit diviser 1, ce qui est impossible

Décomposition en facteurs premiers

Définition : Théorème fondamental de l'arithmétique

$\forall n \geq 2$, n se factorise, de manière unique, en un produit de puissances de premiers :

$$n = p_1^{e_1} \dots p_r^{e_r}$$

avec p_i premier et $e_i \geq 0$ entier, où $i \in [1, r]$

Théorème 1

Soit (a, b) le plus grand commun diviseur entre a et b, alors (a, b) est le plus petit élément positif de l'ensemble I où $I = \{ax + by$ tels que $x, y \in \mathbb{Z}\}$

Preuve : Soit d le plus petit élément positif de l'ensemble I ; d est donc de la forme $d = au + bv$ avec u et v appartenant à $\mathbb{Z}$.

Question 1 : d divise-t-il a ? Si d ne divise pas a, nous avons $a = dq + r$ où d est le quotient, r le reste et $0 < r < d$. Ainsi nous avons $r = a - dq$, donc $r = a - (au + bv)q$, et ainsi :

$$r = a(1 - uq) + b(-vq)$$

Cette équation présente r comme une combinaison linéaire de a et b à coefficients entiers, donc $r \in I$ avec $0 < r < d$. Nous avons ainsi une contradiction car d a été choisi comme étant le plus petit élément positif de I et ici $r < d$. Donc d divise a, et de la même manière d divise b.

Théorème 1 (suite)

Question 2 : d est-il le plus grand de tous les diviseurs ? Soit d' un diviseur commun de a et b. d' divise a et d' divise b. Donc d' divise au et d' divise bv. Donc d' divise $au + bv = d$. Donc d' divise $d \Rightarrow d' \leq d$ et $d = (a, b)$.

Conclusion : nous avons montré que d divise a et b et qu'il est le plus grand commun diviseur de a et de b. Ainsi $(a, b) = d$ est le plus petit élément positif de I.

Bézout

Théorème de Bézout
Si $a, b \in \mathbb{Z}$ ne sont pas simultanément nuls, alors il existe u et $v \in \mathbb{Z}$ tels que $au + bv = (a, b)$ où (a, b) dénote le plus grand commun diviseur entre a et b

Preuve :
Découle directement du théorème :
$pgcd(a, b)$ est le plus petit élément positif de l'ensemble I où $I = \{ax + by$ tels que $x, y \in \mathbb{Z}\}$

Inverse modulaire

Théorème : $ax \equiv 1 \pmod{m} \Leftrightarrow (a, m) = 1$

Preuve :

$\boxed{\Rightarrow}$ Nous avons $ax \equiv 1 \pmod{m}$ et donc m divise $ax - 1$. Si $(a, m) = d$, alors d divise a et d divise m ; et si d divise m et m divise $ax - 1$ alors d divise $ax - 1$. Mais comme d divise a, nous avons que d doit diviser 1, et donc d ne peut valoir que 1 : $(a, m) = 1$.

$\boxed{\Leftarrow}$ Si $(a, m) = 1$, par Bézout nous avons qu'il existe u et $v \in \mathbb{Z}$ tels que $au + mv = 1$. Ainsi il existe un u tel que $au \equiv 1 \pmod{m}$ (preuve d'existence de l'inverse). De plus, si $ax_0 \equiv 1 \pmod{m}$ et si $ax_1 \equiv 1 \pmod{m}$ alors $ax_0 - ax_1 \equiv 0 \pmod{m}$ et $a(x_0 - x_1) \equiv 0 \pmod{m}$. Donc m divise $a(x_0 - x_1)$, mais comme $(a, m) = 1$, m doit diviser $x_0 - x_1$ et ainsi par la définition d'une congruence nous avons $x_0 \equiv x_1 \pmod{m}$ (preuve de l'unicité de l'inverse).

Théorème 2

Soit p un nombre premier et soit $(a, p) = 1$ alors les valeurs de a, $2a$, ..., $(p-1)a$ calculées modulo p sont toutes différentes

En effet, si $ia \equiv ja \pmod{p}$ pour $i \neq j$ appartenant tous deux à $[1, p-1]$, alors nous avons que p divise $(i-j)a$

Mais comme $|i-j| < p$, nous avons que $i-j$ est premier avec p. Donc p ne divise pas $i-j$ et ainsi p devrait diviser a, ce qui est une contradiction

Donc $ia \not\equiv ja \pmod{p}$ pour $i \neq j$ appartenant tous deux à $[1, p-1]$ et ainsi :

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots p-1 \pmod{p}$$

Le petit théorème de Fermat

Le petit Théorème de Fermat :
Si m est premier et $(a, m) = 1$ alors $a^{m-1} \equiv 1 \pmod{m}$

Preuve : Supposons que $(a, m) = 1$. Nous pouvons écrire la suite de valeurs : a, $2a$, ..., $(m-1)a$. Aucun de ces $m - 1$ éléments n'est divisible par m. De plus ces $m - 1$ éléments sont tous différents modulo m ; ainsi $i \cdot a \mod m$ pour i allant de 1 à $m - 1$ donne $m - 1$ valeurs différentes plus petites que m Ainsi nous avons :

$$a \cdot 2a \ldots (m-1)a \equiv 1 \cdot 2 \ldots (m-1) \pmod{m}$$

$$a^{m-1}(m-1)! \equiv (m-1)! \pmod{m}$$

$$(a^{m-1} - 1)(m-1)! \equiv 0 \pmod{m}$$

Comme $(m - 1)!$ n'est pas nul, nous avons :
$a^{m-1} \equiv 1 \pmod{m}$

Théorème 3

$$(x, p) = (x \text{ mod } p, p)$$

En effet, si x mod $p = y$ alors il existe un entier l tel que $x = lp + y$.

Ainsi nous avons : $(x, p) = (lp + y, p) = d$ avec d divisant $lp + y$ et divisant p

Puisque d divise p alors d divise lp, mais comme nous avons aussi que d divise $lp + y$, nous avons que d divise y

Comme d divise y et p, nous avons $(y, p) = d$ car d est le plus grand de ces diviseurs, en effet s'il existait un $d' > d$ tel que d' divise p et y, alors ce d' divise aussi lp et donc ce serait un $d' > d$ qui diviserait $lp+y$ ce qui est une contradiction avec $(lp + y, p) = d$.

Ainsi $(x, p) = (x \text{ mod } p, p)$

Fonction Phi d'Euler

Définition : La fonction d'Euler $\Phi(n)$ égale le nombre d'éléments plus petits que n et qui sont premiers avec n

Si n se décompose en facteurs premiers tels qu'indiqué à la définition précédente, nous avons :

$$\Phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Fonction Phi d'Euler (suite)

Théorème : Si $n = p_1^{e_1} \cdots p_r^{e_r}$, nous avons :

$$\phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Preuve :

A Pour un p premier, nous avons $\phi(p) = p - 1$

B Si on travaille modulo p^α, où p est un premier et α est un entier plus grand ou égal à 2, le nombre d'éléments qui ont un diviseur commun avec p^α sont les multiples de p : $1p$, $2p$, ..., $p^{\alpha-1}p$. Il y a donc $p^{\alpha-1}$ multiples de p. Et ainsi :

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$$

Fonction Phi d'Euler (suite)

C Soient m et n de la forme p^α où α est un entier plus grand ou égal à 1 et tels que $(m, n) = 1$. Combien d'éléments plus petits ou égaux à mn sont premiers avec mn ?

Ecrivons les valeurs de 1 à mn sous forme matricielle de la manière suivante :

$$\begin{pmatrix} 1 & 2 & 3 & \dots & m \\ m+1 & m+2 & m+3 & \dots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \dots & 3m \\ \vdots & & & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \dots & nm \end{pmatrix}$$

Une colonne r de cette matrice est composée d'éléments $im+r$ pour i allant de 0 à $n-1$. Si $(r, m) = 1$ alors tous ces éléments $im + r$ d'une telle colonne r sont premiers avec m. En effet, nous avons $(im+r, m) = (im+r \bmod m, m) = (r, m) = 1$. Il y a ainsi $\phi(m)$ valeurs possibles pour r pour avoir $(r, m) = 1$. Il y a donc $\phi(m)$ colonnes composées d'éléments tous premiers avec m.

Fonction Phi d'Euler (suite)

Des éléments composants ces $\phi(m)$ colonnes composées d'éléments premiers avec m, il faut extraire les éléments qui sont aussi premiers avec n. Nous cherchons donc des éléments de la forme $im + r$, pour i allant de 0 à $n - 1$, qui sont premiers avec n. Nous savons que, pour i allant de 0 à $n - 1$, $(im + r, n) = (im + r \bmod n, n)$. Nous remarquons que $im + r \not\equiv jm + r \pmod{n}$ pour $i \neq j$ tous deux allant de 0 à $n - 1$. En effet, si $im + r \equiv jm + r \pmod{n}$ pour $i \neq j$ tous deux allant de 0 à $n - 1$, alors n divise $(i - j)m$. Mais comme $|i - j| < n$, n ne divise pas $i - j$. Donc n devrait diviser m ce qui est une contradiction (car $(m, n) = 1$). Donc quand i varie de 0 à $n - 1$, $im + r$ mod n donne n résultats différents strictement inférieurs à n, à savoir 0, 1, 2, ..., $n - 1$. Il y a donc $\phi(n)$ de ces n valeurs qui sont premières avec n, et ce dans chacune des $\phi(m)$ colonnes considérées.
Donc $\phi(mn) = \phi(m)\phi(n)$

Fonction Phi d'Euler (suite)

D En combinant les points B et C, nous avons que si

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

alors

$$\phi(n) = p_1^{e_1}(1-\frac{1}{p_1}) \ldots p_r^{e_r}(1-\frac{1}{p_r}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Théorème d'Euler

Théorème : soit un groupe formé de $\phi(n)$ éléments, où $n > 2$. Pour un élément a appartenant à ce groupe, nous avons : $a^{\Phi(n)} = 1$

Preuve : Soit $P = a_1 a_2 \dots a_{\phi(n)}$ où les différents a_i appartiennent au groupe considéré. Soit a un élément appartenant aussi au groupe, et calculons :

$$(a \cdot a_1)(a \cdot a_2) \dots (a \cdot a_{\phi(n)})$$

D'un côté nous voyons que cela vaut : $a^{\phi(n)} a_1 \dots a_{\phi(n)} = a^{\phi(n)} P$. D'un autre côté on note que $a \cdot a_i \neq a \cdot a_j$ $\forall i \neq j$. Et comme il y a $\phi(n)$ éléments dans ce produit, nous avons : $(a \cdot a_1)(a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) = a_1 a_2 \dots a_{\phi(n)} = P$.

En conclusion, nous avons $a^{\phi(n)} P = P$ et donc $a^{\phi(n)} = 1$.

Théorème 4

Théorème : Soit a un élément du groupe formé de $\phi(n)$ éléments, l'ordre de a divise l'ordre du groupe.

Preuve : Si l'ordre de l'élément a ne divise par l'ordre du groupe, égal à $\phi(n)$, alors $\phi(n) = q \cdot \text{ordre}(a) + r$ avec $0 < r < \text{ordre}(a)$. Ainsi :

$$a^{\phi(n)} = a^{\text{ordre}(a) \cdot q} a^r = 1^q a^r = a^r$$

Comme $a^r \neq 1$ puisque $r < \text{ordre}(a)$, nous devrions avoir $a^{\phi(n)} \neq 1$, ce qui est une contradiction.

Théorème 5

Théorème : $a \in Q_n \Leftrightarrow a \in Q_p$ et $a \in Q_q$ (où $n = pq$ et p, q sont des premiers distincts)

Preuve :

a est un résidu quadratique modulo n

$\Leftrightarrow$ il existe un x tel que $x^2 \equiv a \pmod{n}$

$\Leftrightarrow x^2 \equiv a(up+vq) \pmod{n}$ (par Bézout, où $up+vq = 1$)

$\Leftrightarrow x^2 \equiv aup + avq \pmod{n}$

$$\Leftrightarrow \begin{cases} x^2 \equiv a \ (p) \\ x^2 \equiv a \ (q) \end{cases}$$ (par le Lemme Chinois)

$\Leftrightarrow a \in Q_p$ et $a \in Q_q$