I Nombres premiers

1) Définition et premières propriétés

Def 1

Un entier p est premier ssi ses seuls diviseurs positifs sont 1 et p.

On note $\mathbb{P}$ l'ensemble des nombres premiers.

Rq 2

- $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\} \subset \mathbb{N}$
- $1 \notin \mathbb{P}$

Prop 3

Il existe une infinité de nombres premiers.

Rq 4

Pour $p \in \mathbb{P}$, on dit que p est un nombre premier :

- de Fermat si il existe $n \in \mathbb{N}$, $p = 2^{2^n} + 1$

ex: $p = 3$ pour $n = 0$

- de Mersenne si il existe $n \in \mathbb{N}$, $p = 2^n + 1$

ex: $p = 3$ pour $n = 2$, $p = 7$ pour $n = 3$

- jumeau si $p + 2 \in \mathbb{P}$

ex: 11 et 13 nombres premiers jumeaux

À l'heure actuelle, on ne sait pas si il existe une infinité ou non de nombres premiers de Fermat, de Mersenne ou jumeaux.

Prop 5

$\forall a > 1$ entier, $\exists!$ suite de nombres premiers $p_1, \dots, p_k$ tels que $a = p_1 p_2 \dots p_k$ et $p_1 \leq p_2 \leq \dots \leq p_k$

ex: $12 = 2 \times 2 \times 3$

2) Nombres premiers entre eux

Def 6

Deux entiers p et q sont premiers entre eux ssi 1 est leur seul diviseur commun.

On note $p \wedge q = 1$.

ex: $2 \wedge 3 = 1$, plus généralement $\forall n \in \mathbb{N}$, $n \wedge (n+1) = 1$

Prop 7 (Lemme de Gauss)

a, b, c entiers non nuls.

Si a divise bc et $a \wedge b = 1$, alors a divise c.

Prop 8 (Lemme de Bezout)

$p \wedge q = 1 \Leftrightarrow \exists u, v \in \mathbb{N}$, $up + vq = 1$

ex: $15 \times 15 - 7 \times 32 = 1$ donc $15 \wedge 32 = 1$

3) Anneau $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, anneau où les règles de calcul s'effectuent modulo n (on note $[n]$).

Def 9

On dit qu'un groupe G est cyclique ssi $\exists a \in G$, tel que $G = \{\dots, a^{-n}, \dots, a^{-1}, e, a, a^2, \dots, a^n, \dots\}$

Prop 10

Soit G cyclique fini de cardinal n. Alors G est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Prop 11

$\bar{m}$ générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1$
$\Leftrightarrow m$ inversible dans $\mathbb{Z}/n\mathbb{Z}$

ex: 5 génère $\mathbb{Z}/6\mathbb{Z}$, car $5 \times 5 = 25 \equiv 1 [6]$, mais 4 ne génère pas $\mathbb{Z}/6\mathbb{Z}$, car $4 \times 3 = 12 \equiv 0 [6]$.

Prop 12 (Lemme chinois)

$$\begin{vmatrix} m \wedge n = 1 \\ m, n \geq 2 \end{vmatrix} \Rightarrow \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

ex: $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Def 13

On appelle indicatrice d'Euler la fonction $\phi : \mathbb{N}^* \to \mathbb{N}$ définie par $\phi(n) = \mathrm{Card}(\mathbb{Z}/n\mathbb{Z}^*)$

ex: $\phi(6) = \text{Card}(\{1,5\}) = 2$

Prop 14
- $\forall p \in \mathbb{P}, \forall \alpha \in \mathbb{N}^*, \phi(p^\alpha) = p^{\alpha-1}(p-1)$
- $\forall m, n \in \mathbb{N}^*, m \wedge n = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$

On dit que ϕ est une fonction multiplicative.

Prop 15
$\forall n \in \mathbb{N}^*$, on note $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la décomposition de n en facteurs premiers (unique à ordre près des facteurs).
Alors $\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

II Les corps $\mathbb{F}_p$ et $\mathbb{F}_{p^\alpha}$

1) Corps $\mathbb{F}_p$

Prop 16
$\forall n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n \in \mathbb{P}$
On note alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Prop 17 (Lemme de Fermat)
$\forall p \in \mathbb{P}, \forall a \in \mathbb{N}, a \wedge p = 1$, on a $a^{p-1} \equiv 1 [p]$

Prop 18
Soit $p \in \mathbb{P}$
- $\forall k \in [\![1, p-1]\!]$, $\binom{p}{k} \equiv 0 [p]$
- $\forall P, Q \in \mathbb{F}_p[X]$, $(P+Q)^p = P^p + Q^p$ et $(P(X))^p = P(X^p)$

Prop 19
Soit K un corps fini. Alors K^* est cyclique.
En particulier, $\forall p \in \mathbb{P}$, $\mathbb{F}_p^*$ est cyclique et possède $p-1$ éléments.

Rq 20
- Il n'existe pas d'algorithme général efficace pour trouver un générateur de $\mathbb{F}_p^*$.
- Ce résultat reste valable pour tout sous-groupe fini d'un corps quelconque.

2) Corps finis

Prop 21
Un corps fini est de caractéristique $p \in \mathbb{P}$. De plus, $\exists \alpha \in \mathbb{N}^*$, $\text{Card}(K) = p^\alpha$.

Prop 22
Les éléments de $\mathbb{F}_{p^\alpha}$ sont les racines du polynôme $X^{p^\alpha} - X \in \mathbb{F}_p[X]$, i.e. $X^{p^\alpha} - X = \prod_{a \in \mathbb{F}_{p^\alpha}} (X - a)$

Prop 23 (Théorème de Wilson)
$\forall n \geq 2$, $n \in \mathbb{P} \Leftrightarrow (n-1)! \equiv -1 [n]$

3) Carrés dans $\mathbb{F}_p^*$

Def 24
$x \in \mathbb{F}_p^*$ est un carré ssi $\exists y \in \mathbb{F}_p^*$, $x = y^2$

Def 25 (Symbole de Legendre)

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 [p] \\ 1 & \text{si } a \text{ carré non nul modulo } p \\ -1 & \text{sinon} \end{cases}$$

Prop 26
On a les propriétés suivantes, pour $a, b \in \mathbb{N}$:
(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
(ii) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) [p]$
(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Rq 27
L'application $\chi : \mathbb{F}_p^* \to \{-1, 1\}$, $a \mapsto \left(\frac{a}{p}\right)$ est un morphisme de groupe

Prop 28
L'ensemble des carrés de $\mathbb{F}_p^*$ est un groupe à $\frac{p-1}{2}$ éléments.
De plus, $\forall a \in \mathbb{F}_p^*$,
- a est un carré $\Leftrightarrow a^{\frac{p-1}{2}} = 1$
- a n'est pas un carré $\Leftrightarrow a^{\frac{p-1}{2}} = -1$

Prop 29 (Théorème de Frobenius-Zolotarev)
Soit V un ev sur $\mathbb{F}_p$ et $u \in GL(V) \subset \mathfrak{S}_V$.
Alors $\varepsilon(u) = \left(\frac{\det u}{p}\right)$ avec ε la signature.

Prop 30 (Loi de réciprocité quadratique)
Soit p, q premiers impairs distincts.
Alors $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

HP

ex : 3 est-il un carré modulo 17 ?
On a $17 \equiv 2[3]$ qui n'est pas un carré, et $(-1)^{\frac{3-1}{2}\frac{17-1}{2}} = 1$
donc $\left(\frac{3}{17}\right) = -1$, 3 n'est pas un carré dans $\mathbb{Z}/17\mathbb{Z}$.

III Applications

1) Cryptographie

App 31 : Système RSA (envoi de message crypté à clef publique)

- On choisit $p, q \in \mathcal{P}$ très grand, et on note $N = pq$.
- On choisit $d \in \mathcal{P}$ tel que $d \wedge \phi(N) = 1$, où $\phi(N) = (p-1)(q-1)$
- On rends publique la clef (N, d)
- Pour envoyer un message $(a_1, \dots, a_n)$ avec $a_i \leq N$, on applique $F(a) = a^d [N]$
- Pour décoder le message, $F^{-1}(b) = b^e [N]$ où $ed \equiv 1 [\phi(N)]$

Rq 32 : Tests de primalité

- Algorithme du Crible : $\not{1}, ②, ③, \not{4}, ⑤, \not{6}, ⑦, \not{8}, \not{9}, \not{10}, \dots$ (on entoure p puis on raye les multiples de p) → définition par récurrence pas efficace
- Théorème de Wilson : $(n-1)!$ trop long à calculer
- Théorème de Fermat et raffinements (on teste des $a \in \mathbb{N}$)

$$\begin{cases} N \text{ premier} \\ a \wedge N = 1 \\ (N = 2^s m \text{ avec } m \text{ impaire}) \end{cases}$$

① ⟹ $a^{N-1} \equiv 1 [N]$
⚠ Si N non-premier, N nombre de Carmichaël

② ⟹ $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) [N]$ (calculé avec la loi de réciprocité quadratique)
Pour k tests, $P(N \text{ premier}) \geq 1 - 2^{-k}$

(Rabin-Miller) ③' ⟹ $a^m \equiv 1 [N]$ ou $\exists r \in [\![0, s-1]\!]$, $a^{2^r m} \equiv -1 [N]$
Pour k tests, $P(N \text{ premier}) \geq 1 - 4^{-k}$

2) Réduction modulo p

Prop 33
Soit $P \in \mathbb{Z}[X]$, $p \in \mathcal{P}$ tq $p \nmid cd(P)$
Si $\bar{P}/(p)$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, **alors** P est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ si $\mathcal{C}(P) = 1$

ex : • $X^2 + X + 1$ irréductible sur $\mathbb{Q}$ car irréductible sur $\mathbb{Z}/2\mathbb{Z}$
• $X^p - X - 1$ irréductible sur $\mathbb{Q}$ car irréductible sur $\mathbb{Z}/p\mathbb{Z}$

Prop 34 (Eisenstein)
Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$ tel que $\begin{cases} p \mid a_i \ \forall i \in [\![0, r-1]\!] \\ p^2 \nmid a_0 \\ p \nmid a_r \end{cases}$

Alors P irréductible dans $\mathbb{Q}[X]$, et si $\mathcal{C}(P) = 1$, de même dans $\mathbb{Z}[X]$

ex : $P = \sum_{k=1}^{p-1} X^k = \frac{X^p - 1}{X - 1}$ irréductible dans $\mathbb{Z}[X]$

3) Application aux équations diophantiennes

La réduction modulo p donne des conditions d'existence de solutions de certaines équations diophantiennes.

ex : • $x^3 - 3xy^2 + y^3 = 7$ dans $\mathbb{Z}$ n'a pas de solution
• $x^3 + 115 y^5 = 137$ n'a pas de solution dans $\mathbb{Z}$
• $11^x = 2^y - 1$ n'a pas de solution dans $\mathbb{Z}$

Prop 35 (Théorème de Sophie-Germain)
Soit $(x, y, z) \in \mathbb{Z}$ vérifiant $x^p + y^p = z^p$ avec p premier vérifiant les conditions suivantes :
$\exists q$ premier tel que • $x^p + y^p = z^p [q] \Rightarrow x, y$ ou $z \equiv 0 [q]$
• $u^p \not\equiv p [q]$ pour $u \in \mathbb{Z}$
Alors p divise x, y ou z.

IV Répartition des nombres premiers

Def 36
$\forall x \in \mathbb{R}$, on note $\pi(x) = \mathrm{Card}(\{p \in \mathcal{P}, p \leq x\})$

Prop 37
$\exists c_1, c_2 > 0$, $c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}$

Prop 38 (admis) : Théorème des nombres premiers
$\pi(x) \sim_{\infty} \frac{x}{\ln x}$

Prop 39
Il existe une infinité de $p \in \mathcal{P}$, $p \equiv 1 [n]$ $(\forall n \geq 2)$

Prop 40 (admis) : Théorème de progression arithmétique de Dirichlet
Soit $a, b \geq 2$, $a \wedge b = 1$
Il existe une infinité de $p \in \mathcal{P}$, $p = a + bn$ $\forall n \in \mathbb{N}^*$

Prop 41 : Postulat de Bertrand
$\forall n \geq 2$, $\exists p \in \mathcal{P}$, $n < p \leq 2n$) DEV

Rq 42
Le théorème de Bertrand implique qu'il existe une infinité de $p \in \mathcal{P}$

Livres :
- Livre (...métique)
- Hindry (« Arithmétique »)
- Aigner (« Proofs from the Book »)
- Cassini (« 1ère année X-ENS, Algèbre 1 »)

Théorème de Frobenius-Zolotarev

Théorème 1. ***Frobenius-Zolotarev***
Soient p un nombre premier impair, et V un espace vectoriel de dimension n sur F_p. Soit $u \in GL(V)$. En regardant u comme une permutation de V, alors on a :

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

Avec $\epsilon(u)$ la signature de u.

Démonstration. La démonstration se décompose en 3 étapes.

1. On montre que $D(GL(V))$ le groupe dérivé de $GL(V)$ coïncide avec $SL(V)$.
2. On en déduit l'existence d'un morphisme surjectif f de F_p^* dans $\{-1, 1\}$ qui vérifie $f \circ det = \epsilon$.
3. On conclut en remarquant qu'il existe un unique morphisme surjectif de F_p^* dans $\{-1, 1\}$, qui coïncide donc avec le symbole de Legendre.

Etape 1 : $D(GL(V)) = SL(V)$.

L'inclusion $D(GL(V)) \subset SL(V)$ est évidente car le determinant d'un commutateur vaut 1. Pour l'inclusion réciproque, on se rappelle que $SL(V)$ est engendré par les transvections. Il suffit de montrer qu'une transvection est un commutateur. Soit $u = Id + \lambda E_{i,j}$ avec $i \neq j$ et $\lambda \in F_p^*$ une transvection. $u^2 = Id + 2\lambda E_{i,j}$ est encore une transvection car on est en caractéristique $p > 2$. Les transvections sont conjuguées entre elles donc il existe $p \in GL(V)$ tel que $u^2 = pup^{-1}$, ou encore $u = pup^{-1}u^{-1}$, qui est bien un commutateur. [Per]

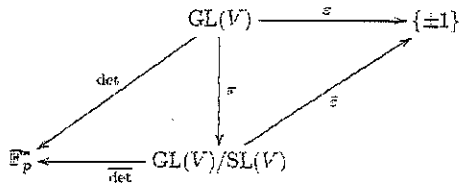
Etape 2 : Existence d'un morphisme f de de F_p^* dans $\{-1, 1\}$ tel que $f \circ det = \epsilon$.

On fait deux observations.

— Le morphisme signature ϵ de $GL(V)$ dans $\{-1, 1\}$ (qui est un groupe abélien) se factorise à travers le quotient $GL(V)/D(GL(V))$ en un morphisme $\overline{\epsilon}$.

— Par propriété universelle du quotient, le morphisme determinant de noyau $SL(V)$ induit un isomorphisme entre $GL(V)/SL(V)$ et F_p^* noté $\overline{\det}$.

On a alors le diagramme commutatif suivant :



L'application $f = \overline{\epsilon} \circ \overline{det}^{-1}$ est un morphisme de F_p^* dans $\{-1,1\}$ qui vérifie $f \circ det = \epsilon$. Montrons que f n'est pas trivial. On va exhiber un $u \in GL(V)$ tel que $\epsilon(u) = f(det(u)) = -1$. V est isomorphe à F_q comme F_p-espace vectoriel (avec $q = p^n$).

Soit ω un générateur de F_q^*. L'application $u : x \mapsto \omega x$ est une application F_p-linéaire qui agit comme la permutation $(\omega, \omega^2, \ldots, \omega^{q-1})$. C'est un cycle de longueur $q-1$ donc de signature $(-1)^q = -1$ car q est impair.

Etape 3 : Unicité d'un morphisme surjectif de F_p^* dans $\{-1,1\}$.

Comme F_p^* est cyclique et $2|p-1$, il contient un unique sous groupe H d'indice 2. Soit g un morphisme surjectif de F_p^* dans $\{-1,1\}$. $|Im(g)| = 2$ donc $[F_p^* : Ker(g)] = 2$ et nécessairement $Ker(g) = H$. Ainsi g est défini de manière intrinsèque par :

$$g(x) = \begin{cases} 1 & \text{si } x \in H \\ -1 & \text{si } x \notin H \end{cases}$$

L'application de $\left(\frac{\cdot}{p}\right)$ de F_p^* dans $\{-1,1\}$ est un morphisme surjectif (il y a exactement $(p-1)/2$ carrés et $(p-1)/2$ non-carrés). Par unicité, ce morphisme coïncide avec le morphisme f défini à l'étape 2. Pour $u \in GL(V)$ on en déduit $\epsilon(u) = f(\det(u)) = \left(\frac{\det(u)}{p}\right)$, ce qui conclut la preuve. □

Remarque.

Soit $\alpha \in F_p^*$ et u le morphisme de multiplication par α dans F_p. Alors $\epsilon(u) = \left(\frac{a}{p}\right)$. C'est une conséquence du théorème précédent pour $V = F_p$.

Soit $u : x \mapsto x^p$ l'automorphisme de Frobenius de F_q ($q = p^n$). On a alors $\epsilon(u) = (-1)^{\frac{(p-1)(n+1)}{2}}$. C'est une conséquence du théorème précédent pour $V = F_q$. Dans une base adaptée, u est une matrice de permutation circulaire de determinant $(-1)^{n+1}$.

Bibliographie

[Per] : PERRIN D., 1996. *Cours d'algèbre.* Ellipses
[Bec] : BECK, MALIK, PEYRÉ, 2004. *Objectif Agrégation.* HK

Postulat de Bertrand

Théorème. *Pour tout entier naturel non nul n, il existe un nombre premier p tel que*

$$n < p \leq 2n$$

Démonstration. On décompose la preuve en 4 étapes.

Étape 1. On montre d'abord le résultat pour $n \leq 4000$ à la main. Chaque terme de la suite de nombres premiers suivante est inférieur a deux fois son prédécesseur. Ainsi pour $n \leq 4000$, il existe p tel que $n < p \leq 2n$.

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

Étape 2. On montre l'inégalité suivante : Soit $x \in \mathbb{R}$. Alors

$$\prod_{p \leq x,\ p \in \mathcal{P}} p \leq 4^{x-1}$$

Remarque. Dorénavant, afin d'alléger les notations, on notera

$$\prod_{p \leq x,\ p \in \mathcal{P}} p = \prod_{p \leq x} p$$

Démonstration. Il suffit de montrer la propriété pour x un nombre premier. En effet, si q désigne le plus grand nombre premier inférieur à x, on a :

$$\prod_{p \leq x} p = \prod_{p \leq q} p \quad \text{et} \quad 4^{q-1} \leq 4^{x-1}$$

Pour $q = 2$ on obtient $2 < 4$. Montrons par récurrence sur la suite de nombre premiers l'inégalité. Soit $q = 2m+1$ un nombre premier et supposons la propriété vraie pour tout entier $k < q$. On a :

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \prod_{m+1 < p \leq 2m+1} p$$

Par hypothèse de récurrence, le premier produit vérifie :

$$\prod_{p \leq m+1} p \leq 4^m$$

Remarquons de plus que le deuxième produit vérifie :

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m}$$

En effet, $\binom{2m+1}{m+1} = \frac{(2m+1)!}{m!(m+1)!}$ est un entier, et les nombres premiers apparaissant dans le produit de gauche sont tous facteurs de $(2m+1)!$ sans être facteur de $m!$ et $(m+1)!$. Enfin on a :

$$\binom{2m+1}{m} \leq 2^{2m}$$

Car :

$$\binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m} \leq \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}$$

On obtient donc l'inégalité suivante :

$$\prod_{p \leq q} p = \prod_{p \leq m+1} p \prod_{m+1 < p \leq 2m+1} p \leq 4^m 2^{2m} = 4^{q-1}$$

Ce qui achève la récurrence.

□

Étape 3. On cherche à encadrer $\binom{2n}{n}$. Soit p un nombre premier. On rappelle la formule de Legendre qui donne la valuation p-adique de la factorielle d'un entier :

$$\nu_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

On a alors :

$$\nu_p\left(\binom{2n}{n}\right) = \nu_p((2n)!) - 2\nu_p(n!) = \sum_{k \geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

Chaque terme de la somme vaut 0 ou 1, puisque :

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2$$

De plus, le terme vaut 0 dés que $p^k > 2n$. Ainsi :

$$\sum_{k \geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \max\{r \in \mathbb{N} \mid p^r \leq 2n\}$$

On en déduit que la plus grande puissance de p divisant $\binom{2n}{n}$ est plus petite que $2n$ **(1)**. En particulier, les nombres premiers supérieurs à $\sqrt{2n}$ apparaissent au plus une fois dans $\binom{2n}{n}$ **(2)**.

De plus, les nombres premiers p vérifiant $\frac{2}{3}n < p \leq n$ ne divisent pas $\binom{2n}{n}$ **(3)**. En effet, $3p > 2n$ implique que p et $2p$ sont les seuls multiples de p apparaissant dans le numérateur de $\frac{(2n)!}{n!^2}$, sachant que nous avons déjà 2 facteurs p dans le dénominateur.

On a les inégalités suivantes :

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p$$

L'inégalité de droite découle des remarques **(1)**, **(2)** et **(3)** qui précèdent. Pour l'inégalité de gauche, on remarque que $\sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}$. Le terme maximal de cette somme est atteint pour $k = n$, donc $\binom{2n}{n}$ est supérieur à la moyenne des termes de la somme, soit $\frac{4^n}{2n}$.

Étape 4 On suppose par l'absurde qu'il n'y a pas de nombre premier p tel que $n < p \leq 2n$. Le produit de droite dans la somme vaut alors 1. Comme il n'y a pas plus de $\sqrt{2n}$ nombres premiers $p \leq \sqrt{2n}$, on obtient :

$$4^n \leq (2n)^{1+\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p$$

Puis en utilisant le résultat démontré plus haut par récurrence :

$$4^n \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n}$$

Ou encore :

$$2^{\frac{2}{3}n} \leq (2n)^{1+\sqrt{2n}}$$

Mais cette inégalité est fausse pour n assez grand. En effet, pour a entier supérieur à 2 on a $a + 1 < 2^a$ (par récurrence). Alors

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 < 2^{6\sqrt[6]{2n}}$$

Pour $n \geq 50$, auquel cas $18 < 20 \leq 2\sqrt{2n}$, on obtient en partant de notre inégalité :

$$2^{2n} \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}$$

Ainsi, $(2n)^{1/3} < 20$, soit $n < 4000$. Ceci conclut la preuve. □

Bibliographie

[Aig] : AIGNER M., ZIEGLER G., 2003. *Proofs from THE BOOK*, Troisième édition. Springer