Théorème 12.13. Bertrand

Pour tout entier naturel non nul n, il existe des nombres premiers compris entre n et $2n$.

Preuve. Pour $1 \leq n \leq 4$ c'est clair. Supposons que, pour un entier $n \geq 5$, il n'existe pas de nombre premier compris entre n et $2n$. Dans ce cas, on a $]n, 2n[\cap \mathcal{P} = \emptyset$ et l'inégalité (12.6) devient $2^{\frac{2n}{3}} \leq (2n)^{\sqrt{2n}}$, ce qui est équivalent à $\frac{2n}{3}\ln(2) \leq \sqrt{2n}\ln(2n) = 2\sqrt{2n}\ln\left(\sqrt{2n}\right)$, soit à $\frac{\ln\left(\sqrt{2n}\right)}{\sqrt{2n}} \geq \frac{\ln(2)}{6}$. Nous sommes donc conduit à étudier la fonction définie pour $x \geq 5$ par $f(x) = \frac{\ln(x)}{x}$. Sa dérivée $f'(x) = \frac{1-\ln(x)}{x^2}$ s'annule pour $x = e$ et f est strictement décroissante sur $]e, +\infty[$, à valeurs strictement positives et nulle à l'infini.

Avec $\frac{\ln(30)}{30} - \frac{\ln(2)}{6} \backsim -2.1 \times 10^{-3} < 0$ (et $\frac{\ln(29)}{29} - \frac{\ln(2)}{6} \backsim 5.8 \times 10^{-4} > 0$), on déduit que $\frac{\ln\left(\sqrt{2n}\right)}{\sqrt{2n}} < \frac{\ln(2)}{6}$ pour tout $n \geq 5$ tel que $\sqrt{2n} < 30$, soit pour $n < \frac{30^2}{2} = 450$. On donc ainsi montré que pour tout entier $n \geq 450$, il existe des nombres premiers entre n et $2n$.

Pour les entiers compris entre 5 et 450, il n'est pas nécessaire de considérer tous les cas. On peut remarquer que la suite de nombres premiers :

$$(q_k)_{1\leq k\leq 9} = (5, 7, 13, 23, 43, 83, 163, 317, 631)$$

est telle que $q_k < q_{k+1} < 2q_k$. Il en résulte que pour $5 \leq n \leq 450$, tout intervalle $]n, 2n]$ contient l'un de ces nombres premiers. En effet, en désignant pour $n \geq 5$, par k le plus grand indice tel que $q_k \leq n$, on a $q_k \leq n < q_{k+1} < 2q_k \leq 2n$ et $q_{k+1} \in]n, 2n]$. □

12.5 Quelques tests de primalité

Pour tout entier $n \geq 2$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est l'anneau des classes résiduelles modulo n et $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ le groupe multiplicatif des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$. On se reportera au chapitre 11 pour une étude détaillée de ces anneaux ainsi que de la fonction indicatrice d'Euler que nous utiliserons.

Le théorème qui suit nous donne quelques critères de primalité.

Théorème 12.14.

Pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :

1. *n est premier ;*
2. *pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\,n^{\alpha-1}$;*
3. *$\varphi(n) = n - 1$;*

4. *n est premier avec tout entier compris entre 1 et $n-1$;*
5. *$\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps ;*
6. *$\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est intègre ;*
7. *$(n-1)! \equiv -1 \pmod{n}$ (théorème de Wilson) ;*
8. *$(n-2)! \equiv 1 \pmod{n}$;*
9. *pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;*
10. *$n = 2$ ou n est impair et $\left(\left(\dfrac{n-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{n+1}{2}} \pmod{n}$;*
11. *pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$;*
12. *pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$;*
13. *il existe un entier relatif a premier avec n tel que $(X+\overline{a})^n = X^n + \overline{a}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}[X]$.*

Preuve. On vérifie d'abord que les assertions (1) à (6) sont équivalentes.

(1) $\Rightarrow$ (2) Supposons que n soit premier. Un entier k compris entre 1 et n^α n'est pas premier avec n^α si, et seulement si, il est divisible par n, ce qui équivaut à dire qu'il existe un entier q compris entre 1 et $n^{\alpha-1}$ tel que $k = qn$ et cela nous donne $n^{\alpha-1}$ possibilités. Il en résulte que $\varphi(n^\alpha) = n^\alpha - n^{\alpha-1} = (n-1)\,n^{\alpha-1}$.

(2) $\Rightarrow$ (3) Il suffit de prendre $\alpha = 1$.

(3) $\Leftrightarrow$ (4) Dire que $\varphi(n) = n-1$ revient à dire que tous les éléments de $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\overline{0}\}$ sont inversibles, ce qui équivaut encore à dire que tous les entiers compris entre 1 et $n-1$ sont premiers avec n.

(4) $\Rightarrow$ (5) Si tous les entiers compris entre 1 et $n-1$ sont premiers avec n, on a alors $\varphi(n) = n-1$, donc $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times = \dfrac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\overline{0}\}$, ce qui revient à dire que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps.

(5) $\Rightarrow$ (6) Résulte du fait qu'un corps est en particulier un anneau intègre.

(6) $\Rightarrow$ (1) Supposons que l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ soit intègre. Si d est un diviseur de n différent de n dans $\mathbb{N}^*$, il existe alors un entier q compris entre 2 et n tel que $n = qd$ et dans l'anneau intègre $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ on a $\overline{q}\overline{d} = \overline{0}$ avec $\overline{d} \neq \overline{0}$, ce qui impose $\overline{q} = \overline{0}$, soit $q = n$ et $d = 1$. L'entier n est donc premier.

On prouve l'équivalence entre (1) et (7), soit le théorème de Wilson.

(1) $\Rightarrow$ (7) Pour n premier, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps et tout élément $\overline{k}$ de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ est racine du polynôme $X^{n-1}-\overline{1}$, donc $X^{n-1}-\overline{1}=\prod_{k=1}^{n-1}\left(X-\overline{k}\right)$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}[X]$ et en évaluant ce polynôme en $\overline{0}$, il vient $-\overline{1}=\prod_{k=1}^{n-1}\left(-\overline{k}\right)=(-1)^{n-1}\,\overline{(n-1)!}=\overline{(n-1)!}$ (pour $n=2$, on a $(-1)^{n-1}=-\overline{1}=\overline{1}$ et $n\geq 3$ premier est impair, donc $(-1)^{n-1}=\overline{1}$).

(7) $\Rightarrow$ (1) Si $n\geq 2$ est tel que $\overline{(n-1)!}=-\overline{1}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, alors tout diviseur d de n compris entre 1 et $n-1$ divisant $(n-1)!=-1+kn$ va diviser -1, ce qui impose $d=1$ et l'entier n est premier.

(7) $\Leftrightarrow$ (8) Pour $n\geq 2$, on a $(n-1)!=(n-1)\,(n-2)!\equiv -(n-2)!$ modulo n.

(7) $\Leftrightarrow$ (9) L'implication (9) $\Rightarrow$ (7) est évidente ($k=1$). Supposons que $(n-1)!\equiv -1\ (n)$. Dans ce cas, n est premier.
Si $n=2$, on a alors, pour $k=1$ et $k=2$:

$$(n-k)!\,(k-1)!=1\equiv(-1)^k\pmod 2$$

Pour $n\geq 3$ qui est premier impair, on procède par récurrence finie sur k.
Le résultat est acquis pour $k=1$ et pour $k=n$ (puisque $(-1)^n=-1$). En supposant le résultat acquis pour $k\in\{1,\cdots,n-2\}$, on a :

$$(n-(k+1))!k!=\frac{k}{n-k}\,(n-k)!\,(k-1)!$$

avec $\overline{n-k}=-\overline{k}$ qui est inversible dans le corps $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ puisque $\overline{k}\neq\overline{0}$, ce qui nous donne l'égalité dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$:

$$\overline{(n-(k+1))!k!}=\frac{\overline{k}}{\overline{-k}}\,\overline{(n-k)!\,(k-1)!}=-\overline{(-1)^k}=\overline{(-1)^{k+1}}$$

soit $(n-(k+1))!k!\equiv(-1)^{k+1}\pmod n$.

(7) $\Leftrightarrow$ (10) Pour $n=2q+1\geq 3$ et k entier compris entre 1 et q, on a :

$$q+k=n-q-1+k\equiv-(q+1-k)\pmod n$$

donc :

$$\begin{aligned}(n-1)!=(2q)!&=1\cdot 2\cdot\cdots\cdot(q-1)\cdot q\cdot(q+1)\cdot\cdots\cdot(2q)\\&\equiv(1\cdot 2\cdot\cdots\cdot(q-1)\cdot q)\cdot((-q)\cdot(-(q-1))\cdot\cdots\cdot(-1))\pmod n\\&\equiv(-1)^q\,(q!)^2\pmod n\end{aligned}$$

soit $(n-1)!\equiv(-1)^{\frac{n-1}{2}}\left(\left(\dfrac{n-1}{2}\right)!\right)^2\pmod n$. Il en résulte que :

$$\begin{aligned}&((n-1)!\equiv -1\pmod n)\\&\Leftrightarrow\left(n=2\text{ ou }n\text{ est impair et }\left(\left(\frac{n-1}{2}\right)!\right)^2\equiv(-1)^{\frac{n+1}{2}}\pmod n\right)\end{aligned}$$

(1) $\Rightarrow$ (11) Si $n \geq 2$ est premier, comme il divise $n! = k!\,(n-k)!\binom{n}{k}$ et est premier avec $k!\,(n-k)!$ (sinon il diviserait ce produit et donc l'un des entiers j compris entre 1 et $n-1$, ce qui est impossible), il divise $\binom{n}{k}$ (théorème de Gauss), ce qui revient à dire que $\binom{n}{k} \equiv 0 \pmod{n}$.

(11) $\Rightarrow$ (12) Supposons que $\binom{n}{k} \equiv 0 \pmod{n}$ pour tout entier k compris entre 1 et $n-1$. Pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ (triangle de Pascal), donc $\binom{n-1}{k} \equiv -\binom{n-1}{k-1} \pmod{n}$ et par récurrence sur k compris entre 0 et $n-1$, on déduit que $\binom{n-1}{k}$ est congru à $(-1)^k$ modulo n. En effet, on a $\binom{n-1}{0} = 1 \equiv (-1)^0 \pmod{n}$ et $\binom{n-1}{1} = n-1 \equiv -1 \pmod{n}$, puis en supposant le résultat acquis pour $k-1$ compris entre 0 et $n-2$, on a $\binom{n-1}{k} \equiv -\binom{n-1}{k-1} \equiv -(-1)^{n-1} = (-1)^k \pmod{n}$. Enfin on termine avec l'équivalence de (1), (12) et (13).

(12) $\Rightarrow$ (1) Supposons que $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$ pour tout entier k compris entre 1 et $n-1$. Pour tout diviseur k de n compris entre 1 et $n-1$, on a $0 \equiv \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} \equiv \frac{n}{k}(-1)^{k-1} \pmod{n}$ (pour $k=1$, on a bien $\binom{n-1}{0} = 1 \equiv (-1)^0$ modulo n), ce qui impose $k=1$ (sinon n divise $\frac{n}{k} \in \{2, \cdots, n-1\}$, ce qui est impossible), donc n est premier.

(1) $\Rightarrow$ (13) Si n est premier, on a alors $\binom{n}{k} \equiv 0 \pmod{n}$, pour tout k compris entre 1 et $n-1$, ce qui implique en utilisant la formule du binôme de Newton que, que pour tout entier $a \in \mathbb{Z}$, on a $(X+\overline{a})^n = X^n + \overline{a}^n$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}[X]$, puis le théorème de Fermat nous dit que $\overline{a}^n = \overline{a}$.

(13) $\Rightarrow$ (1) S'il existe a premier avec n tel que $(X+\overline{a})^n = X^n + \overline{a}$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}[X]$, on a alors $\binom{n}{k}a^k \equiv 0$ modulo n pour tout k compris entre 1 et $n-1$ et $a^n \equiv a$ modulo n. Comme n est premier avec a et divise $\binom{n}{k}a^k$, pour k compris entre 1 et $n-1$, il va diviser $\binom{n}{k}$ (théorème de Gauss), donc n est premier.

□

Pour $p \geq 2$ premier, le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est noté $\mathbb{F}_p$.