§2. Préliminaires de théorie des nombres

de la fonction puissance,

ou du prédicat de résiduation quadratique,

ou de restrictions faibles soit de l'addition, soit de la multiplication, soit de la division.

L'article se conclut au § 10 sur des perspectives d'étude de la conjecture par les méthodes de codage, mais aussi sur une réflexion de logicien tentant de comprendre l'éventuel caractère « désespéré » de certaines conjectures arithmétiques comme celle qui nous intéresse.

§ 2. Préliminaires de théorie des nombres

2.1. On note $\mathbf{N}$, $\mathbf{Z}$, P les ensembles respectivement formés des entiers naturels, des entiers rationnels, et des nombres premiers.

L'ensemble des diviseurs premiers de x est appelé *support* de x et noté SUPP (x).

Un outil essentiel est le *Théorème de Dirichlet* sur l'infinitude des premiers dans les progressions arithmétiques $u(n) = an + b$, pour $a \perp b$. Joint au *Théorème des restes chinois*, il conduit à l'existence d'une infinité de solutions en entiers premiers des systèmes de congruences du type

$$z \equiv s_1 \pmod{t_1}, \ldots, z \equiv s_n \pmod{t_n}$$

où $t_1, \ldots, t_n$ sont deux à deux premiers entre eux et $0 < s_1 < t_1, \ldots, 0 < s_n < t_n$.

2.2. Un résultat constamment utilisé dans ce qui suit est le Théorème découvert par K. Zsigmondy en 1892, et redécouvert ensuite par Birkhoff et Vandiver en 1904, que nous appelons Théorème ZBV et que voici :

Théorème (Zsigmondy-Birkhoff-Vandiver). *Soient x et y des entiers premiers entre eux tels que $0 < y < x$. Pour tout $n > 0$, il existe au moins un diviseur premier de $x^n - y^n$ qui ne divise pas $x^m - y^m$ pour $0 < m < n$ (un tel diviseur est dit* primitif *pour $x^n - y^n$) excepté dans les cas suivants :*

i) $n = 1, x - y = 1$, *$x - y$ n'a alors aucun diviseur premier ;*

ii) $n = 2, x + y = 2^u$ *où* $u > 0$;

iii) $n = 6, x = 2, y = 1$.

2.3. L'analogue du Théorème ZBV à propos des formes $x^n + y^n$ a été démontré par R. Lucas et R. Carmichael (cf. [CR]).

THÉORÈME (Lucas-Carmichael). *Soient* x *et* y *des entiers premiers entre eux tels que* $0 < y < x$. *Pour tout* $n > 0$, *il existe au moins un diviseur premier de* $x^n + y^n$ *qui ne divise pas* $x^m + y^m$ *pour* $0 < m < n$ *(un tel diviseur est dit* caractéristique *pour* $x^n + y^n$*) excepté dans le cas où* $n = 3, x = 2$ *et* $y = 1$.

Ce théorème est, en fait, corollaire de ZBV puisque tout diviseur primitif de $x^{2n} - y^{2n}$ est diviseur caractéristique de $x^n + y^n$.

2.4. Si p est premier, nous notons $\mathrm{ORD}(x, p)$ l'ordre de x modulo p, c'est-à-dire le plus petit α tel que $x^\alpha \equiv 1 \pmod{p}$.

Il est clair que p divise (resp. est diviseur primitif de) $x^\alpha - 1$ si et seulement si α est multiple de (resp. est égal à) $\mathrm{ORD}(x, p)$.

Les Théorèmes ZBV et LC, joints au fait simple suivant lequel le pgcd des entiers $x^n - 1$ et $x^m - 1$ est $x^{\mathrm{pgcd}(n, m)} - 1$, montrent le résultat suivant:

COROLLAIRE. *Pour tout entier* $x > 1$ *et tous entiers* α *et* β*:*

i) *L'égalité* $\mathrm{SUPP}(x^\alpha - 1) = \mathrm{SUPP}(x^\beta - 1)$ *équivaut à* ($\alpha = \beta$ ou bien x est de la forme $2^u - 1$ avec $u > 1$ et α et β éléments de $\{1, 2\}$).

ii) *L'inclusion* $\mathrm{SUPP}(x^\beta - 1) \subseteq \mathrm{SUPP}(x^\alpha - 1)$ *équivaut à* ($\beta \mid \alpha$ ou x est de la forme $2^u - 1$ avec $u > 1$ et $\beta = 2$).

iii) *Un entier* p *est diviseur primitif de* $x^\alpha - 1$ *si et seulement si* p divise $x^\alpha - 1$ et, ou bien $\alpha = 1$, ou bien $\mathrm{SUPP}(x^\alpha - 1) \subset_{\neq} \mathrm{SUPP}(x^\beta - 1)$ pour tout $\beta \neq \alpha$ tel que p divise $x^\beta - 1$.

iv) *L'égalité* $\mathrm{SUPP}(x^\alpha + 1) = \mathrm{SUPP}(x^\beta + 1)$ *équivaut à* ($\alpha = \beta$ ou bien $x = 2$ et α et β sont éléments de $\{1, 3\}$).

Preuve. Cf. les Corollaires 1.7, 1.8 et 1.9 de [RD1] pages 223-224.

2.5. Le Théorème suivant remonte à C. Størmer (1897, cf. [SC1] et [SC2]).

THÉORÈME (Størmer). *Soient* $p_1, ..., p_n$ *des premiers distincts,* $K, \alpha_1, ..., \alpha_n$ *des entiers strictement positifs. Pour* $1 \leqslant i \leqslant n$, *posons* $\varepsilon_i = 1$ *si* α_i *est impair et* $\varepsilon_i = 2$ *si* α_i *est pair. Posons aussi* $D = K \cdot p_1^{\varepsilon_1} \cdot \ldots \cdot p_n^{\varepsilon_n}$.

Si $x^2 - 1 = K \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ *alors* x *est la solution fondamentale de l'équation de Pell-Fermat* $x^2 - Dy^2 = 1$.

Si $x(x+1) = K \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ *alors* $2x + 1$ *est la solution fondamentale de l'équation de Pell-Fermat* $x^2 - 4Dy^2 = 1$.

COROLLAIRE.

i) *Si* E *est un ensemble de* n *entiers premiers distincts, il y a au plus* 2^n *entiers* x *tels que* $\mathrm{SUPP}[x(x+1)] \subseteq E$.
Ainsi, pour tout entier a, *l'ensemble* $ST(a)$ *des entiers* b *tels que*

$$\mathrm{SUPP}(a) = \mathrm{SUPP}(b) \quad et \quad \mathrm{SUPP}(a+1) = \mathrm{SUPP}(b+1)$$

est lui aussi fini.

ii) *Les entiers naturels* x *et* y *sont égaux si et seulement si les conditions suivantes sont simultanément satisfaites:*

1) $\mathrm{SUPP}(x-1) = \mathrm{SUPP}(y-1)$ *et* $\mathrm{SUPP}(x+1) = \mathrm{SUPP}(y+1)$;

2) *pour tout premier* p *et tout* $i \in \{-1, +1\}$, *les valuations de* p *dans les décompositions primaires de* $x + i$ *et de* $y + i$ *ont la même parité.*

2.6. COROLLAIRE 1. *Soit* A *un ensemble fini d'entiers positifs de même support. Il existe un entier* $N(A)$ *tel que, pour tous* x *et* y *dans* A, *les conditions suivantes soient équivalentes:*

i) $x = y$,

ii) *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad et$$
$$\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1),$$

iii) *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1).$$

iii)bis *Il existe* $m > N(A)$ *tel que*

$$\mathrm{SUPP}(mx-1) = \mathrm{SUPP}(my-1).$$

Preuve. Soit E l'ensemble fini

$$E = \{q \in \mathbf{N}: \text{il existe } (u, v) \in A \times A \text{ tel que } u \neq v \text{ et } q \in \mathrm{SUPP}(|u-v|)\}.$$

Le Théorème de Størmer assure que l'ensemble

$$\{z \in \mathbf{N}: [\mathrm{SUPP}[z(z+1)] \subseteq E\}$$

est fini, majoré par un entier $N(A)$.

Soient x et y des éléments distincts de A, avec $x < y$. Nous montrons que si l'une des conditions ii) ou iii) est vérifiée alors l'entier m est majoré par $N(A)$.

Supposons que l'on ait

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad \text{et} \quad \mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1).$$

Tout diviseur premier q de $x+m$ ou de $x+m+1$ divise alors $y-x$. Ainsi, l'entier $(x+m)(x+m+1)$ a un support inclus dans E et donc — par définition de $N(A)$ — l'entier $x+m$ est majoré par $N(A)$. En particulier, m est majoré par $N(A)$.

Supposons maintenant que l'on ait $\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1)$. Tout diviseur premier q de $mx+1$ divise alors $m(y-x)$ et donc aussi $y-x$. Ainsi, l'entier $mx(mx+1)$ a encore un support inclus dans E et l'entier mx est donc majoré par $N(A)$. En particulier, l'entier m est majoré par $N(A)$.

Le cas où $\mathrm{SUPP}(mx-1) = \mathrm{SUPP}(my-1)$ est analogue.

COROLLAIRE 2. *Soient x et y des entiers positifs ou nuls. Les conditions suivantes soient équivalentes:*

i) $x = y$,

ii) *x et y ont le même support et, pour une infinité d'entiers m, on a*

$$\mathrm{SUPP}(x+m) = \mathrm{SUPP}(y+m) \quad \text{et}$$
$$\mathrm{SUPP}(x+m+1) = \mathrm{SUPP}(y+m+1),$$

iii) *x et y ont le même support et, pour une infinité d'entiers m, on a*

$$\mathrm{SUPP}(mx+1) = \mathrm{SUPP}(my+1).$$

2.7. Il est intéressant de remarquer que, sans utiliser le Théorème de Stømer, un autre résultat du même type peut être prouvé en se servant du Théorème de Dirichlet.

PROPOSITION. *Soit A un ensemble fini d'entiers. Pour chaque x de A, il existe des entiers premiers p arbitrairement grands tels que*

$$\mathrm{SUPP}(px+1) \cap \Big[\bigcup_{y \in A\setminus\{x\}} \mathrm{SUPP}(py+1)\Big] \subseteq \{2\}.$$

Preuve. Soit d le produit des entiers premiers ne divisant pas x et appartenant à la réunion des $\mathrm{SUPP}(|y-z|)$ avec y et z dans A. Soit x' tel que $xx' \equiv 1 \pmod d$. On sait qu'il existe des entiers p arbitrairement grands tels que $p \equiv x' \pmod d$, c'est-à-dire tels que $\mathrm{SUPP}(px-1)$ contienne $\mathrm{SUPP}(d)$. Il nous suffit de montrer que, pour de tels p, on a, pour tout y de $A\setminus\{x\}$

$$\mathrm{SUPP}(px+1) \cap \mathrm{SUPP}(py+1) \subseteq \{2\}.$$

Soit q un diviseur premier de $px + 1$ et $py + 1$. Comme $q \neq p$ et q divise $p\,|x - y|$, alors q divise $|x - y|$. N'étant pas dans SUPP(x), il divise d. Par suite, q divise $px - 1$; comme q divise aussi $px + 1$, on a $q = 2$.

2.8. L'étude des suites d'entiers de même support remonte au moins à G. Pòlya qui prouva un résultat amélioré depuis par M. Langevin (cf. [LM1]).

THÉORÈME.

i) (G. Pòlya) *Si* $(a_n)_{n\in\mathbf{N}}$ *est une suite strictement croissante d'entiers positifs de même support alors la suite* $(a_{n+1}-a_n)_{n\in\mathbf{N}}$ *tend vers l'infini.*

ii) (M. Langevin) *Si* $0 < x < y$ *et* SUPP(x) = SUPP(y), *alors*

$$|y - x| > [\mathrm{Log}\,(x+y)]^{1/6}.$$

Ce résultat permet d'améliorer la condition ii) du Corollaire 2 de 2.6 en montrant que la donnée d'une infinité de supports du type SUPP$(x+i)$ caractérise x.

COROLLAIRE. *Soient* x *et* y *des entiers de* $\mathbf{Z}$.

Si pour une infinité d'entiers $m \in \mathbf{N}$ *on a* SUPP$(|x+m|)$ = SUPP$(|y+m|)$ *alors* $x = y$.

Preuve. Supposons que l'ensemble

$$I = \{i \in \mathbf{N} : \mathrm{SUPP}\,(|x+i|) = \mathrm{SUPP}\,(|y+i|)\}$$

soit infini et que l'on ait $x < y$. Observant qu'un diviseur premier de $x + i$ et $y + i$ divise $y - x$, on constate que SUPP$(|x+i|) \subseteq$ SUPP$(y-x)$. Le principe des tiroirs montre qu'il existe une partie X de SUPP$(y-x)$ telle que l'ensemble $J = \{i \in \mathbf{N} : \mathrm{SUPP}\,(|x+i|) = \mathrm{SUPP}\,(|y+i|)\}$ soit infini. On définit par récurrence une suite strictement croissante d'entiers positifs, tous de support X comme suit:

$a_0 = x+i$ et $a_1 = y+i$ où i est minimum dans J tel que $x+i>0$;

$a_{2n} = x+j$ et $a_{2n+1} = y+j$ où j est minimum dans J tel que $x+j>a_{2n-1}$.

La preuve s'achève en remarquant que $(a_{2n+1}-a_{2n})_{n\in\mathbf{N}}$ est constante de valeur $y - x$ et donc ne tend pas vers l'infini avec n, ce qui contredit le Théorème de Pòlya.

2.9. Nous mentionnons enfin un résultat qui souligne la portée de la conjecture E-W sur $\mathbf{N}$.

En formalisant la négation de cette conjecture, on obtient la formule suivante:

$$\forall k\, \exists x\, \exists y > x\, \forall i \leqslant k \quad [\mathrm{SUPP}(x+i) = \mathrm{SUPP}(y+i)] .$$

Il est intéressant de constater que l'énoncé

$$\forall k\, \exists x\, \exists y > x\, \forall i \leqslant k \quad [\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i)] ,$$

obtenu en remplaçant l'égalité par l'inclusion est facilement prouvable.

PROPOSITION. *Pour tout* $k > 0$, *pour tout* $x \in \mathbf{N}$ *il existe* $y > x$ *tel que*

$$\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i) \quad \textit{pour tout} \quad i \in \{0, 1, ..., k\} .$$

Preuve. On considère le plus grand entier premier p qui divise $(x+k)!$. Un y convenable est alors donné par les conditions $y > x$ et $y \equiv x \pmod{\pi}$, où π est le produit des entiers premiers $q < p$.

Remarque. La condition $y > x$ est ici essentielle. En effet, M. Langevin a montré que si pour tout x assez grand il existe $y < x$ tel que $\mathrm{SUPP}(x+i) \subseteq \mathrm{SUPP}(y+i)$ pour tout $i \in \{0, 1, 2\}$ alors la conjecture d'Oesterlé-Masser est fausse (cf. [LM2]).

2.10. L'étude de la conjecture d'Erdös-Woods introduit naturellement la notion suivante:

Définition. Soit A une partie de $\mathbf{Z}$. On note $\cong_A$ la relation d'équivalence sur $\mathbf{Z}$ définie comme suit:

$x \cong_A y$ si et seulement si $\mathrm{SUPP}(|x+i|) = \mathrm{SUPP}(|y+i|)$ pour tout $i \in A$.

Notons $[x]_A$ la classe de x pour $\cong_A$. Le Fait suivant est immédiat.

FAIT. 1°) *Si* $A \subseteq B$ *alors* $\cong_A$ *est moins fine que* $\cong_B$.
La relation $\cong_\emptyset$ *est l'équivalence grossière.*
2°) *Si* $t \in \mathbf{Z}$, $x \in \mathbf{Z}$, $y \in \mathbf{Z}$, $A + t = \{x + t : x \in A\}$, $-A = \{-x : x \in A\}$, *alors* $x \cong_{A+t} y$ *si et seulement si* $x + t \cong_A y + t$ *(i.e.* $[x]_{A+t} = ([x+t]_A) - t$*);* $x \cong_{-A} y$ *si et seulement si* $-x \cong_A -y$ *(i.e.* $[x]_{-A} = -[-x]_A$*).*
3°) *Si* $x \in \mathbf{Z}$ *alors* $[x]_{\{-x\}} = [x]_{\{-x+1\}} = \{x\}$.

Remarque. 1°) La conjecture d'Erdös-Woods exprime alors simplement qu'*il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{0, 1, ..., k\}}$ *soit la relation d'égalité.*

2°) La conjecture d'Erdös-Woods équivaut aussi aux assertions suivantes:

(E-W)bis *Il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{-k,\ldots,0\}}$ *soit la relation d'égalité.*

(E-W)ter *Il existe une constante* k *telle que la trace sur* $\mathbf{N}$ *de la relation* $\cong_{\{-k,\ldots,k\}}$ *soit la relation d'égalité.*

Seules les implications (E-W)ter $\Rightarrow$ (E-W) et (E-W)ter $\Rightarrow$ (E-W)bis sont non triviales.

La première résulte facilement de l'égalité $[x]_{\{0,\ldots,2k\}} = [x+k]_{\{-k,\ldots,k\}} - k$. La seconde résulte de l'égalité $[x]_{\{-2k,\ldots,0\}} = [x-k]_{\{-k,\ldots,k\}} + k$ pour $x \geqslant k$, et des égalités $[x]_{\{-2k,\ldots,0\}} = \{x\}$ pour $x < k$.

2.11. Le Corollaire 2.8 et le théorème de Størmer 2.6 se traduisent par le théorème suivant:

THÉORÈME.

i) *Si* A *est infini alors* $\cong_A$ *est la relation d'égalité sur* $\mathbf{Z}$.

ii) *Les classes d'équivalence de* $\cong_A$ *sont finies dès que* A *contient deux entiers successifs de* $\mathbf{Z}$.

iii) *Si* A *contient un segment* $\{i,\ldots,i+k\}$ *de* $\mathbf{Z}$, $x \cong_A y$ *et* $x \neq y$ *alors*

$$|x-y| \geqslant \prod_{p\in P,\, p|(x+i)\ldots(x+i+k)} p \quad \geqslant \quad \prod_{p\leqslant k+1,\, p\in P} p\ .$$

Preuve. i) Supposons $A \cap \mathbf{N}$ infini et $x \cong_A y$.

Soit $m \in \mathbf{N}$ tel que $x+m > 0$ et $y+m > 0$. Comme $(A-m) \cap \mathbf{N}$ est aussi infini et que $x+m \cong_{A-m} y+m$, le Corollaire 2.8 assure l'égalité $x+m = y+m$ et donc $x = y$. Dans le cas où $A \cap (\mathbf{Z}\backslash\mathbf{N})$ est infini on considère $\cong_{-A}$ et on conclut à l'aide du point 2 du Fait 2.10.

ii) Notons $[x]_A$ la classe de x pour $\cong_A$.

Le théorème de Størmer montre que les traces de $[x]_{\{0,1\}}$ et $[x]_{\{-1,0\}}$ sur $\mathbf{N}$ et $\mathbf{Z}\backslash\mathbf{N}$ sont finies. D'après le point 2 du Fait 2.10 on a $[x]_{\{0,1\}} = ([x]_{\{0,1\}} \cap \mathbf{N}) \cup (-([-x]_{\{-1,0\}} \cap \mathbf{N}))$, égalité qui montre le caractère fini des classes de $\cong_{\{0,1\}}$. On conclut la preuve de ii) à l'aide du point 2 du Fait 2.10, en considérant les $\cong_{A+t}$.

iii) Il suffit d'observer que si p divise $x+j$ il divise aussi $y+j$ et donc $x-y$.

2.12. Les points i) et iv) du Corollaire 2.4 se traduisent par le théorème suivant:

THÉORÈME. *Les restrictions à l'ensemble PP des entiers primaires des relations* $\cong_{\{0,1,2\}}$, $\cong_{\{-2,-1,0\}}$ *et* $\cong_{\{-1,0,1\}}$ *coïncident avec la relation d'égalité. Les parties des* PP^k, $k > 0$, *sont donc saturées pour les relations d'équivalence* $\cong_A$ *telles que A contienne* $\{0, 1, 2\}$ *ou bien* $\{-2, -1, 0\}$ *ou bien* $\{-1, 0, 1\}$.

Preuve. Le point iv) du Corollaire 2.4 montre que la seule classe de $\cong_{\{0,1\}}$ dont la trace sur *PP* n'est pas réduite à un seul élément est celle de 2 dont la trace est $\{2, 8\}$. Comme $\mathrm{SUPP}(2+2) = \{2\}$ et $\mathrm{SUPP}(8+2) = \{2, 5\}$, on voit que $2 \not\cong_{\{0,1,2\}} 8$.

Le point i) du Corollaire 2.5 montre que les seules classes de $\cong_{\{-1,0\}}$ dont les traces sur *PP* ne sont pas réduites à un seul élément sont les classes $\{p, p^2\}$ où p est un entier premier de Mersenne, i.e. de la forme $p = 2^u - 1$. Comme $p^2 + 1 = (2^u-1)^2 + 1 = 2[2^u(2^{u-1}-1)+1]$, on voit que $\mathrm{SUPP}(p^2+1) \neq \{2\}$ tandis que $\mathrm{SUPP}(p+1) = \mathrm{SUPP}(2^u) = \{2\}$, d'où $p \not\cong_{\{-1,0,1\}} p^2$. Comme $p - 2 = 2^u - 3$ et $p^2 - 2 = (2^u-3)(2^u+1) + 2$, ces entiers sont impairs et premiers entre eux, d'où $p \not\cong_{\{-2,-1,0\}} p^2$.

Le Fait 2.10 donne le corollaire suivant de ce Théorème:

COROLLAIRE. *Soit* $n > 0$. *Sur l'ensemble* $PP + [0, n] = \{x + s : x \in PP$ *et* $0 \leqslant s \leqslant n\}$ *la relation* $\cong_{\{-n-1,\ldots,-1,0\}}$ *coïncide avec la relation d'égalité.*

Sur l'ensemble $PP + [-n, 0] = \{x + s : x \in PP$ *et* $-n \leqslant s \leqslant 0$ *et* $x + s \geqslant 0\}$ *la relation* $\cong_{\{0,1,\ldots,n+1\}}$ *coïncide avec la relation d'égalité.*

Sur l'ensemble $PP + [-n, n]$ *la relation* $\cong_{\{-n,\ldots,0,\ldots,n\}}$ *coïncide avec la relation d'égalité.*

Les parties des $(PP+[0, n])^k$ *(resp.* $(PP+[-n, 0])^k$, *resp.* $(PP+[-n, n])^k$*) où* $k > 0$, *sont donc saturées pour les relations d'équivalence* $\cong_A$ *telles que A contienne* $\{-n-1, \ldots, 0\}$ *(resp.* $\{0, \ldots, n+1\}$, *resp.* $\{-n, \ldots, 0, \ldots, n\}$*).*

Remarques. 1°) Soit U l'ensemble

$$U = \{-56, -26, -20, -14, -11, -10, -6, -5, -4, 0, 1, 4, 10, 16, 46\}.$$

On peut montrer (en utilisant le Théorème ZBV) que la restriction de $\cong_{\{0,1,m\}}$ à l'ensemble *PP* des entiers primaires coïncide avec la relation d'égalité si et seulement si $m \notin U$.

2°) Les cas d'exception du Théorème ZBV étant liés aux premiers de Mersenne, il semble plus difficile de déterminer les m pour lesquels la relation $\cong_{\{0,-1,m\}}$, restreinte à *PP*, coïncide avec l'égalité: ce sont les m tels que, pour tout Mersenne p on ait $\mathrm{SUPP}(p+m) \neq \mathrm{SUPP}(p^2+m)$.

Outre la valeur $m = -2$ vue dans le Théorème précédent, on peut montrer que c'est le cas des entiers $m = \pm q^\alpha - 1$, où q est un premier non Mersenne, $m \notin \{-p^2 - p : p$ est Mersenne et $p^2 + p - 1$ est premier$\}$ et $m \notin \{-6, -5\}$ (à cause de $p = 3$). Les exemples de tels m entre -20 et 22 sont

$$-20, -18, -17, -14, -12, -10, -9, -8, -5, -4, -3, 1, 2, 4,$$
$$6, 8, 10, 12, 15, 16, 18, 22.$$

On peut aussi montrer qu'en revanche, outre 0 et -1, les valeurs suivantes de m ne conviennent pas:

— les entiers $-57, -27, -21, -15, -12, -11, -7, -6, -5, 3, 9, 15, 45$ (à cause de $p = 3$),

— les entiers $-2695, -385, -343, -336, -133, -105, -91, -70, -63, -56, -55, -43, -35, -31, -28, -25, -21, -13, 5, 7, 14, 35, 49, 140, 252, 287, 329, 2639$ (à cause du Mersenne 7),

De façon générale, pour chaque Mersenne p, ne conviennent pas:

— les entiers $m = r(p-1) - p$, où SUPP $[(r(r+p)] \subseteq$ SUPP $(p-1)$, entiers qui sont premiers avec p. En particulier, pour $r = -1, -p-1, -p+1$ on obtient $-p^2 - p + 1, -p^2 + p - 1$ et $-2p + 1$).

— les entiers $m = p[r(p-1)-1]$ où SUPP $[(r(r+1)] \subseteq$ SUPP $[p(p-1)]$. En particulier, on peut prendre $r = -9, -4, -3, -2, 1, 2, 3, 8, p, -p, p-1, -p-1, p^2-1, -p^2$, d'où les valeurs suivantes de m:

$$-p[p^2(p-1)+1], -p^3, -p[p(p-1)+1], -p(9p-8), -p(4p-3),$$
$$-p(3p-2), -p(2p-1), -p(p+2), -p(p+1), p, p^2, p(p-2), p(2p-3),$$
$$p(3p-4), p(8p-9), p(2p-3), p[p(p-1)+1], p^2(p-2)+1, p[(p+1)(p-1)^2-1].$$

etc.

2.13. Le symbole de Legendre qui indique qu'un entier x est résidu quadratique modulo un entier premier p est noté $\left(\frac{x}{p}\right)$.

Nous aurons besoin au § 7 du lemme suivant, combinaison du *critère d'Euler* (qui caractérise les résidus quadratiques modulo les premiers) et du Théorème de Dirichlet:

LEMME. *Soit x un entier impair et p un diviseur premier de x. Il existe un entier premier q, qui ne divise pas x, tel que* $\left(\frac{p}{q}\right) = -1$

et $\left(\frac{p'}{q}\right) = +1$ *pour tout* $p' \in \mathrm{SUPP}(x)\backslash\{p\}$.

Par suite, $\left(\frac{x}{q}\right) = (-1)^{\alpha}$, *où* α *est l'exposant de* p *dans la décomposition primaire de l'entier* x.

Preuve. Soit s l'un des $(p-1)/2$ entiers qui ne sont pas résidus quadratiques modulo l'entier p. Considérons le système de congruences suivant:

$$z \equiv 1 \pmod 4, \quad z \equiv 1 \pmod{x/p^{\alpha}}, \quad z \equiv s \pmod p.$$

Le Théorème des restes chinois et le Théorème de Dirichlet montrent qu'il existe un entier premier $q > x$ solution de ce système.

Soit $p' \in \mathrm{SUPP}(x)\backslash\{p\}$. Comme $q > x$, on a $q \neq p'$. D'autre part, puisque $q \equiv 1 \pmod 4$, on voit que l'entier $(q-1)(p'-1)/4$ est pair pour tout $p' \in \mathrm{SUPP}(x)\backslash\{p\}$. La loi de réciprocité quadratique assure donc

$$\left(\frac{p'}{q}\right) = \left(\frac{q}{p'}\right).$$

La condition $q \equiv s \pmod p$ conduit à $\left(\frac{q}{p}\right) = \left(\frac{s}{p}\right) = -1$ puisque s n'est pas un résidu quadratique modulo p. Ainsi, on a $\left(\frac{p}{q}\right) = -1$. La condition $q \equiv 1 \pmod{p'}$ nous assure que $\left(\frac{p'}{q}\right) = \left(\frac{q}{p'}\right) = +1$. Le caractère multiplicatif du symbole de Legendre montre alors que:

$$\left(\frac{x}{q}\right) = \left(\frac{p^{\alpha}}{q}\right) \times \left(\frac{x/p^{\alpha}}{q}\right) = (-1)^{\alpha},$$ ce qui achève la démonstration.

2.14. Nous aurons besoin au § 9 de caractériser l'égalité en termes de division vue modulo un entier fixé. Si $v > 0$, nous notons $\mathrm{Quot}(u, v)$ et $\mathrm{Reste}(u, v)$ les quotient et reste de la division euclidienne de u par v.

LEMME. *Soient* x, y, α *des entiers positifs ou nuls. Si* $\alpha \geqslant 3$ *et* $y - x \geqslant 2$ *alors il existe un entier premier* $p \neq \alpha$ *tel que* $p\mathrm{Quot}(x, p) \not\equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$.

Preuve. 1°) Des inégalités $\mathrm{Quot}(t, p) \leqslant t/p < \mathrm{Quot}(t, p) + 1$ on déduit

$$|\mathrm{Quot}(y, p) - \mathrm{Quot}(x, p)| - 1 < |y - x|/p < |\mathrm{Quot}(y, p) - \mathrm{Quot}(x, p)| + 1.$$

On a donc

$$|\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| - 1 \leqslant \operatorname{Quot}(|y-x|,p) < |\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| + 1,$$

d'où

$$\operatorname{Quot}(|y-x|,p) = |\operatorname{Quot}(y,p) - \operatorname{Quot}(x,p)| + \varepsilon, \quad \text{où} \quad \varepsilon \in \{-1, 0\}.$$

2°) Nous traitons d'abord le cas où $y - x \geqslant 8$. Nous utiliserons le Théorème de Tchebycheff sur l'existence d'un premier strictement compris entre x et $2x$ (ceci pour $x \geqslant 2$).

Si $y - x \geqslant 8$ alors il existe des premiers p et q tels que $(y-x)/4 < q < (y-x)/2 < r < y - x$. On a donc $2 < (y-x)/q < 4$, $1 < (y-x)/r < 2$, d'où $\operatorname{Quot}(y-x, q) = 1$ et $\operatorname{Quot}(y-x, r) = 3$.

Le point 1°) montre alors que

$$\operatorname{Quot}(y,r) - \operatorname{Quot}(x,r) = 1 - \varepsilon \in \{1, 2\}$$
$$\text{et} \quad \operatorname{Quot}(y,q) - \operatorname{Quot}(x,q) = 1 - \varepsilon \in \{3, 4\}.$$

3°) On déduit de ce qui précède que

$$q\operatorname{Quot}(x,q) - q\operatorname{Quot}(y,q) \in \{3q, 4q\} \quad \text{et} \quad r\operatorname{Quot}(x,r) - r\operatorname{Quot}(y,r) \in \{r, 2r\}$$

Observons que $\{2, 3, 4, q, 2q, 3q, 4q\} \cap \{2, r, 2r\} = \{2\}$ car r et q sont premiers et $2 < q < r$. Comme $\alpha \neq 2$, on voit que les deux cas suivants sont exhaustifs.

1er cas : $\alpha \notin \{2, 3, 4, q, 2q, 3q, 4q\}$.

L'entier α ne divise alors ni $3q$ ni $4q$. On peut choisir pour p l'entier q puisque $q \neq \alpha$ et $q\operatorname{Quot}(y,q) - q\operatorname{Quot}(x,q) \not\equiv 0 \pmod{\alpha}$.

2e cas : $\alpha \notin \{2, r, 2r\}$.

L'entier α ne divise alors ni r ni $2r$. On peut choisir pour p l'entier r puisque $r \neq \alpha$ et $r\operatorname{Quot}(y,r) - r\operatorname{Quot}(x,r) \not\equiv 0 \pmod{\alpha}$.
Ceci achève la preuve dans l'hypothèse $y - x \geqslant 8$.

4°) Supposons maintenant $y = x + 2$. Comme $\alpha \geqslant 3$ on a $2\operatorname{Quot}(y,2) - 2\operatorname{Quot}(x,2) = 2 \not\equiv 0 \pmod{\alpha}$ et on peut prendre pour p l'entier 2.

5°) Supposons maintenant $y = x + i$, i premier, $i \geqslant 3$ (ce qui règlera les cas $y - x = 3, 5, 7$). On a alors $i\operatorname{Quot}(y,i) - i\operatorname{Quot}(x,i) = i$.
Si $\alpha \neq i$ alors on peut choisir pour p l'entier i.
Si $\alpha = i$ alors $2\operatorname{Quot}(y,2) - 2\operatorname{Quot}(x,2) \in \{2[i/2], 2([i/2]+1)\}$, ensemble

qui ne contient pas i car i est un premier impair. Ainsi, on peut choisir pour p l'entier 2.

6°) Supposons maintenant $y = x + 4$. On a alors

$$2\mathrm{Quot}(y, 2) - 2\mathrm{Quot}(x, 2) = 4 .$$

Si $\alpha \neq 4$ alors on peut choisir pour p l'entier 2 (car on a toujours $\alpha \neq 2$).
Si $\alpha = 4$ alors $3\mathrm{Quot}(y, 3) - 3\mathrm{Quot}(x, 3) \in \{3, 6\}$, ensemble qui ne contient pas 4. On peut alors choisir pour p l'entier 3.

7°) Supposons enfin $y = x + 6$. On a alors $2\mathrm{Quot}(y, 2) - 2\mathrm{Quot}(x, 2) = 6$ et $5\mathrm{Quot}(y, 5) - 5\mathrm{Quot}(x, 5) \in \{5, 10\}$. Comme $\alpha \neq 2$, α ne peut pas diviser 6 et l'un d'entre 5 et 10. Ainsi, on peut donc prendre pour p l'une au moins des valeurs 2 ou 5.

Le Lemme précédent permet d'établir le résultat suivant:

PROPOSITION. *Soient* x, y, α *des entiers positifs ou nuls.*

1°) *Les conditions suivantes sont équivalentes:*

i) $x = y$.

ii)$_\alpha$ (*où* $\alpha \geqslant 3$) $\mathrm{Reste}(x, p) \equiv \mathrm{Reste}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$.

iii)$_\alpha$ (*où* $\alpha \geqslant 3$) $\mathrm{Quot}(x, p) \equiv \mathrm{Quot}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$ *et* $|y - x| \neq 1$.

iv)$_\alpha$ (*où* $\alpha \geqslant 3$) $p\mathrm{Quot}(x, p) \equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$ *pour tout premier* $p \neq \alpha$ *et* $|y - x| \neq 1$.

Preuve de la Proposition.

1°) Le Lemme précédent se traduit immédiatement par l'implication iv)$_\alpha \Rightarrow$ i).

2°) Observons que si $p > z$ alors $\mathrm{Reste}(z, p) = z$. Ainsi, considérant un premier p supérieur à α, x et y, on voit que ii)$_\alpha$ implique $x \equiv y \pmod{\alpha}$.

3°) L'égalité $x = p\mathrm{Quot}(x, p) + \mathrm{Reste}(x, p)$ montre immédiatement que si

$$x \equiv y \pmod{\alpha} \quad \text{et} \quad \mathrm{Reste}(x, p) \equiv \mathrm{Reste}(y, p) \pmod{\alpha}$$

alors
$$p\mathrm{Quot}(x, p) \equiv p\mathrm{Quot}(y, p) \pmod{\alpha} .$$

Par ailleurs, la condition $x \equiv y \pmod{\alpha}$ implique $|y - x| \neq 1$.
Ceci montre que ii)$_\alpha \Rightarrow$ iv)$_\alpha$.

4°) On conclut en remarquant que les implications i) $\Rightarrow$ ii)$_\alpha$, i) $\Rightarrow$ iii)$_\alpha$, iii)$_\alpha \Rightarrow$ iv)$_\alpha$ sont toutes triviales.

Remarques. 1°) La restriction $|y - x| \neq 1$, triviale dans ii)$_\alpha$, ne peut être omise dans iii)$_\alpha$. En fait, les conditions suivantes sont équivalentes:

A) $y = x + 1$ et $p\mathrm{Quot}(x, p) \equiv p\mathrm{Quot}(y, p) \pmod{\alpha}$ pour tout premier $p \neq \alpha$;

B) $(x, y) = (0, 1)$ ou bien α est premier et $(x, y) = (\alpha^k - 1, \alpha^k)$ pour un $k \geqslant 1$.

2°) Le statut des assertions ii)$_2$, iii)$_2$ et iv)$_2$ reste ouvert. On note cependant qu'elles ne sont équivalentes à i) puisque

$$\mathrm{Quot}(0, p) = \mathrm{Quot}(2, p) = 0 \text{ pour tout premier } p \neq 2 .$$

$$\mathrm{Reste}(0, p) \equiv \mathrm{Reste}(2, p) \pmod{2} \text{ pour tout premier } p .$$

§ 3. Préliminaires de logique

3.1. Les *langages formels logiques* que nous considérerons sont ceux, dits *du premier ordre*, qui ne comportent qu'un seul type de variables. Dans le cadre arithmétique auquel nous nous intéressons, ces variables sont alors destinées à varier sur l'ensemble **N** des seuls entiers naturels et non sur les ensembles, relations ou fonctions sur **N**.

Ainsi, les formules ne permettent de traduire que les seules quantifications sur les entiers et non sur les relations ou fonctions comme il est usuel et tacite de le faire en mathématiques (en particulier dans les définitions par induction).

Un langage logique du premier ordre L est caractérisé par une liste de symboles spécifiques à chacun desquels est attaché un caractère relationnel ou fonctionnel ainsi qu'une arité (i.e. le nombre des arguments). En pratique, on désignera un langage L par la simple liste de ses symboles spécifiques fonctionnels puis relationnels, omettant d'expliciter les arités (rendues évidentes par le contexte).

A partir des variables on construit les termes de L par « composition » des symboles fonctionnels. Par « application » des symboles relationnels aux termes, on obtient les formules atomiques. Les opérations de négation, conjonction, implication et quantifications appliquées aux formules atomiques donnent enfin les formules de L.

3.2. Soit $L = (f_1, ..., f_m; R_1, ..., R_n)$ un langage du premier ordre.

Une *structure* $\Omega = \langle X; \varphi_1, ..., \varphi_m; \rho_1, ..., \rho_n \rangle$ du langage L est la donnée