Ensemble des nombres entiers

1 Nombres entiers naturels

1.1 Définition des nombres entiers naturels

Définition 1. (Ensemble des entiers naturels) *On appelle ensemble des nombres entiers naturels tout ensemble E possédant les propriétés suivantes :*

1. *Il existe une application injective $s : E \longrightarrow E$ appelée fonction de succession. Pout tou élément $e \in E$, $s(e)$ est appelée le successeur de e.*
2. *Il existe un élément de E qui n'est le successseur d'aucun élément de E. Cette élément est appelé zéro et noté 0.*
3. *Le « Principe de récurrence » est satisfait. Soit M la partie de E constituée par les éléments qui possèdent une certaine propriété p. On note « $p(e)$ » le fait que l'élément e possède la propriété p. Le principe de récurrence s'énonce ainsi : **« Si M contient 0 et le successeur de chacun de ses éléments alors $M = E$. »**. Plus formellement, soit $M = \{e \in E | p(e)\}$:*

$$((0 \in M) \wedge (e \in M \Longrightarrow s(e) \in M)) \Longrightarrow (M = E)$$

Remarque. $M = E$ signifie évidemment que la propriété est possédée par tous les entiers naturels. C'est, en général, la conclusion attendue d'un « raisonnement par récurrence ».

Notation 2. *On note $\mathbb{N}$ l'ensemble des entiers naturels. On note respectivement 1 le successeur de 0, 2 le successeur de 1, etc.*

1.2 Quelques avatars du principe de récurrence

Il existe une version « affaiblie » du principe de récurrence : la récurrence restreinte, qui permet de s'assurer qu'une propriété est vraie à partir d'un certain rang...

Proposition 3. (Récurrence restreinte) *Soit $M = \{n \in \mathbb{N} | p(n\}$. Si $m \in M$ et si $(m \in M \Longrightarrow s(m) \in M)$, alors M est de la forme $\{m, m+1, m+2, ...\}$.*

Démonstration. Elle se démontre à partir du principe de récurrence. □

Il existe encore une version « renforcée » : la récurrence généralisée, qui permet de « supposer la propriété vraie jusqu'à l'ordre n »...

Proposition 4. (Récurrence généralisée) *Soit $M = \{n \in \mathbb{N} | p(n\}$. Si $\forall m \in M, \{0, 1, ..., ...m\} \subset M$ et si $s(m) \in M$, alors $M = \mathbb{N}$.*

Démonstration. Elle se démontre à partir du principe de récurrence. □

Remarque. La récurrence généralisée permet d'éviter un double raisonnement par récurrence.

Preuve par récurrence : la méthode. La manière correcte de rédiger un raisonnement par récurrence est la suivante :

1. Soit M l'ensemble des entiers naturels qui vérifient ... (mettre ici l'énoncé de la propriété que l'on cherche à démontrer)
2. **Initialisation de la récurrence :** vérifier que 0 est élément de M (« la propriété est vraie pour $n = 0$ »)
3. **Caractère héréditaire de la propriété :** soit n un élément de M (cela a un sens, puisque l'on sait maintenant que M n'est pas vide : il contient au moins 0), vérifions que $s(n)$ est encore élément de M (« la propriété est vraie pour $n+1$ »)

Exercice 1. Montrer que $\forall n \in \mathbb{N}$, 7 divise $3^{2n+1} + 2^{n+2}$.

Exercice 2. Montrer que $\forall m, n \in \mathbb{N}^*$, $\forall r \in \mathbb{N}$, $m^{2r+1} + n^{2r+1}$ est divisible par $m + n$.

1.3 Opérations et relation d'ordre dans $\mathbb{N}$

On suppose ici connues les opérations et la relation d'ordre classiques qui existent dans $\mathbb{N}$: addition, multiplication, relation d'inégalité au sens large. Ces éléments peuvent être définis rigoureusement, et toutes les propriétés démontrées par récurrence.

Exemple. Par exemple, on peut définir la relation d'ordre sur $\mathbb{N}$ $p \leqslant n$ par : $\exists q \in \mathbb{N}$, $n = p + q$.

Proposition 5. *Les opérations classiques sur $\mathbb{N}$ ont pour propriétés :*

- *l'addition est commutative, associative et 0 en est un élément neutre,*
- *la multiplication est commutative, associative et 1 en est un élément neutre,*
- *la multiplication est distributive sur l'addition,*
- *les entiers naturels sont totalement ordonnés par l'inégalite´, et cette relation d'ordre est compatible avec l'addition et avec la multiplication.*

1.4 Nombres premiers

Définition 6. (Multiple et diviseur) *Si un entier naturel n peut s'écrire sous la forme $n = pq$, où p et q sont des entiers naturels, on dit que n est un multiple de p et que p est un diviseur de n.*

Exercice 3. Soit $m = 2^3 * 5 * 7^2 * 13^3$. Combien le nombre m a-t-il de diviseurs naturels ?

Définition 7. (Nombre premier) *Un nombre premier est un nombre entier naturel strictement supérieur à 1 qui n'est divisible que par 1 et par lui-même.*

Exemple. Ainsi, le plus petit nombre premier (et le seul qui soit pair) est 2.

Proposition 8. *Il existe une infinité de nombres premiers.*

Exercice 4. Démontrer, par l'absurde, la proposition précédente.

Remarque. Le problème de la primalité d'un nombre (très grand, évidemment) est difficile.

Définition 9. (Décomposition en facteurs premiers) *L'écriture d'un entier n sous la forme $n = a^\alpha b^\beta c^\gamma \ldots$, ou $a, b, c, \ldots$ sont les diviseurs premiers distincts de n et où les exposants $\alpha, \beta, \gamma, \ldots$ sont tels que, par exemple, n est divisible par a^α mais pas par $a^{\alpha+1}$ s'appelle la décomposition en facteurs premiers de n.*

On dit que les exposants $\alpha, \beta, \gamma, \ldots$ sont les ordres de multiplicité des diviseurs $a, b, c, \ldots$

Proposition 10. *La décomposition d'un entier en ses facteurs premiers est unique.*

Exercice 5. Écrivez les nombres 3850 et 1980 sous forme de produits de nombres premiers.

Exercice 6. (Nombre de Fermat) On appelle nombres de Fermat les nombres de la forme $F_p = 2^{2^p} + 1$.

1. Montrer que, pour que $2^n + 1$ soit premier, il faut que n soit une puissance de 2.
2. La réciproque n'est pas vraie : donner un exemple de nombre de Fermat qui ne soit pas premier.
3. Montrer que, pour $k \geqslant 1$, F_p divise $F_{p+k} - 2$.
4. En déduire que F_p et F_{p+k} sont premiers entre eux
5. En déduire qu'il existe une infinité de nombres premiers.

1.5 Relation de divisibilité

On a vu dans le chapitre sur les relations entre ensembles la relation binaire de divisibilité définie dans $\mathbb{N}^*$. Cette relation est une relation d'ordre partiel : il existe des paires d'entiers non comparables par cette relation.

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

Exemple. 3 ne divise pas 7 et 7 ne divise pas 3. Ces deux entiers ne sont donc pas comparables du point de vue de la divisibilité.

Cet ordre n'est donc que partiel, mais il existe, pour chaque couple d'entiers distincts, une borne inférieure et une borne supérieure...

Définition 11. (PGCD, PPMC) *Tout ensemble fini de nombres entiers strictement positifs admet une borne supérieure et une borne inférieure pour la relation de divisibilité.*

Cette borne inférieure et cette borne supérieure sont respectivement appelées plus grand commun diviseur et plus petit commun multiple de ces deux entiers. Ils sont respectivement noteés $a \wedge b$ et $a \vee b$.

Remarque 12. L'existence du PGCD découle de l'existence de la décomposition en facteurs premiers : il suffit de comparer les décompositions des deux nombres pour découvrir leur PGCD. Le PPCM, lui, vaut $a \vee b = ab/(a \wedge b)$.

Exemple. Comme $48 = 2^4 3$ et que $56 = 2^3 7$, on voit aisément que $48 \wedge 56 = 2^3$.

Définition 13. (Treillis)

Proposition 14. $\mathbb{N}^*$ *est un treillis pour la divisibilité. On peut de pluus montrer que :*

1. *ce treillis est distributif, c'est à dire que : $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ et que $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,*
2. *1 est un élément minimal de ce treillis, mais il n'existe pas d'élément maximum,*
3. *les nombres premiers sont les éléments minimaux de ($\mathbb{N}^* \backslash \{1\}$).*

Définition 15. *Deux nombres entiers strictement positifs a et b sont dits premiers entre eux lorsque $a \wedge b = 1$.*

Exercice 7. Soient a, b, c, d des entiers naturels non nuls tels que $ad = bc$. Prouvez que si a et b sont premiers entre eux, alors $b|d$.

1.6 Entiers relatifs

L'ensemble habituellement noté $\mathbb{Z}$ des entiers relatifs est obtenu à partir de $\mathbb{N}$ par le procédé de symétrisation pour l'addition. Sans s'étendre sur le sujet, disons que cela consiste à introduire les entiers strictement négatifs comme opposés des positifs correspondants, par $n + (-n) = 0$. On sait que les porpriétés des opérations sont conservées ; la seule propriété perdue dans cette extension est la compatibilté entre la relation d'ordre et la multiplication. En revanche, on gagne évidemment l'existence d'un opposé pour chaque entier.

2 Division euclidienne dans $\mathbb{Z}$ et applications

2.1 Définition

On se donne deux entiers relatifs a et b, b non nul.

Proposition 16. *Il existe un et un seul couple d'entiers relatifs q et r qui vérifient la relation suivante : $a = bq + r$, avec $0 \leqslant r < |b|$.*

Définition 17. (Division euclidienne) *Obtenir les valeurs de q et de r, c'est effectuer la division euclidienne de a par b. q est appelé quotient, r est appelé reste (dans la division euclidienne). Enfin, lorsque r est nul, a est dit divisible par b, ou b est un diviseur de a.*

Exemple. Le quotient et le reste de la division euclidienne de :

1. $m = -38$ par $n = 6$ est $q = -7$ et $r = 4$,
2. $m = 165$ par $n = -14$ est $q = -11$ et $r = 11$.

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

Exercice 8. On se place dans l'ensemble $\mathbb{N}$.

1. Trouver les restes dans la division par 5 du carré d'un entier.
2. Trouver les restes dans la division par 8 du carré d'un entier impair.
3. Trouver les restes dans la division par 11 de 37^n (pour $n \in \mathbb{N}^*$).
4. Montrer que $10^n(9n-1)+1$ est divisible par 9.

2.2 Représentation des nombres entiers

Définition 18. (Principe de la numération de position) *Il consiste à choisir une base b de numération, et b symboles qui constitueront les chiffres dans la représentation d'un entier positif en base b. Celle-ci s'écrira alors*

$$n = n_p b^p + n_{p-1} b^{p-1} + \cdots + n_1 b^1 + n_0$$

Cette écriture est abrégée en $(\overline{n_p n_{p-1} \ldots n_0})_b$

Remarque 19. En informatique, on utilise couramment les bases 2, 8 et 16.

Obtention de cette représentation. L'algorithme pour obtenir la représentation en base b d'un entier est :

1. Effectuer la division euclidienne de cet entier par b, division qui donne un premier quotient et un premier reste.
2. Le quotient est à sont tour divisé par b pour donner un second quotient et un second reste, et ainsi de suite jusqu'à obtenir un quotient nul.
3. Les restes successifs (tous strictement inférieurs à b), et en commençant par le dernier, constituent la représentation en base b de l'entier donné.

Algorithme de Hörner. Réciproquement, étant donnée la représentation en base b d'un entier, on obtient sa valeur par application de l'algorithme de Hörner :

$n = n_p b^p + n_{p-1} b^{p-1} + \cdots + n_1 b^1 + n_0$ est donné par $(.....(((n_p b + n_{p-1})b + n_{p-2})b + \ldots + n_1)b + n_0)$

Exercice 9. (Numération, changement de base)

1. Chercher les entiers dont le carré, en représentation décimale, a mêmes chiffres des dizaines et des unités.
2. On pose $a=2p-1, b=2p+1, c=2p+3$; trouver l'entier p de manière que $a^2+b^2+c^2$ soit de la forme $(\overline{xxxx})_{10}$.
3. L'entier n s'écrit $(\overline{341})_{10}$ et $(\overline{2331})_a$. Trouver a.
4. Montrer que, dans toute base b supérieure ou égale à 3, l'entier qui s'écrit $(\overline{11211})_b$ n'est pas premier.
5. Soit $n \geqslant 7$. Donner l'écriture de $(n+1)^4$ en base n.

Problème 1. (Développement décimal) On considère le nombre réel x dont le développement décimal s'écrit $x=$ 0,012 345 679 012 345 679 ... ... (la séquence 012 345 679 est reproduite indéfiniment). Ce développement décimal est périodique, de période 9.

1. Montrer que x vérifie une équation de la forme $10^k x = n + x$, où k et n sont des entiers à déterminer. En résolvant cette équation, montrer que x est un nombre rationnel, et le mettre sous la forme $x=\frac{p}{q}$, où p et q sont premiers entre eux.
2. Appliquer la même méthode au "nombre" y dont le développement décimal est $y = 0{,}999999999999...$ (périodique de période 1). Quelle conclusion peut-on en tirer ?
3. Démontrer que tout nombre réel dont le développement décimal est fini ou périodique à partir d'un certain rang est un nombre rationnel.
4. Réciproquement, on se propose de démontrer que le développement décimal de tout nombre rationnel est fini ou périodique à partir d'un certain rang. Pour cela, on considère un rationnel $x=\frac{p}{q}$, avec $q>0$, $p \in \mathbb{Z}$, p et q premiers entre eux, et on étudiera successivement les cas suivants :
   - x est entier (c'est à dire $q=1$)
   - x est rationnel non entier, et q est premier avec 10 (On pourra montrer que, si q est premier avec 10, il existe un entier k, non nul, tel que $10^k \equiv 1 \bmod q$).
   - x est rationnel non entier, mais q n'est pas premier avec 10.

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

2.3 Arithmétique modulo n

On rappelle ici la définition de la relation dite de « congruence modulo n » définie dans $\mathbb{Z}$ étudiée dans le chapitre consacré aux relations entre ensembles.

Définition 20. (Congruence modulo n) *Soit n un entier strictement supérieur à 1 et x et y deux éléments de $\mathbb{Z}$. On dit que « x est congru à y modulo n » lorsque x et y possèdent le même reste dans la division euclidienne par n. On note cette relation par :*

$$x = y \bmod n \text{ ou } x \equiv y \bmod n \text{ ou } x = y[n] \text{ ou } x \equiv y[n].$$

Proposition 21. *Soit n un entier strictement supérieur à 1 et x et y deux éléments de $\mathbb{Z}$.*

$$x = y \bmod n \Longleftrightarrow \exists k \in \mathbb{Z}, x - y = kn.$$

Démonstration. **Exercice 10.** □

Proposition 22. *La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration. **Exercice 11.** □

Remarque 23. La classe d'équivalence d'un entier donné comprend donc cet entier et tous ceux qui ont le même reste que lui dans la division euclidienne par n.

Exemple. Si $n = 3$, il y'a trois classe d'équivalence distinctes :

- $\bar{0} = \{..., -6, -3, 0, 3, 6, ...\}$,
- $\bar{1} = \{..., -5, -2, 1, 4, 7, ...\}$,
- $\bar{2} = \{..., -4, -1, 2, 5, 8, ...\}$.

D'une manière générale, pour n quelconque, il y a exactement n classes d'équivalence, notées de $\bar{0}$ à $\overline{(n-1)}$, c'est-à-dire, il faut le remarquer, un nombre fini.

Proposition 24. *L'ensemble-quotient (ensemble des classes d'équivalence) de la relation de congruence modulo n est un ensemble fini à n éléments noté $\mathbb{Z}/n\mathbb{Z}$.*

Exemple. $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Proposition 25. *La relation de « congruence modulo n » est compatible avec l'addition et la multiplication des nombres entiers.*

Démonstration. **Exercice 12.** □

Remarque 26. C'est cette propriété qui permet de définir dans l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ des opérations, dites induites par celles qui existent dans $\mathbb{Z}$...

Définition 27. (Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$) *On définit dans $\mathbb{Z}/n\mathbb{Z}$:*

- *l'addition par : $\bar{x} + \bar{y} := \overline{x+y}$;*
- *la multiplication par : $\bar{x}.\bar{y} := \overline{x.y}$.*

Proposition 28. (L'anneau $\mathbb{Z}/n\mathbb{Z}$) *L'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ verifient les propriétés suivantes :*

1. *L'addition et la multiplication sont commutatives et associatives*
2. *La mutiplication est distributive par rapport à l'addition*
3. *$\bar{0}$ est un élément neutre pour l'addition.*
4. *$\bar{1}$ est un élément neutre pour la multiplication.*

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

On dit que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un* ***anneau unitaire commutatif*** *pour évoquer les propriétés précédentes.*

Démonstration. **Exercice 13.** □

Exemple. C'est ainsi qu'on obtient les tables d'opérations suivantes dans $\mathbb{Z}/4\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Figure 1. Table d'addition de $\mathbb{Z}/4\mathbb{Z}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Figure 2. able de multiplication de $\mathbb{Z}/4\mathbb{Z}$

Remarque 29. On aperçoit la présence de « diviseurs de zéro » $\bar{2}\times\bar{2}=\bar{0}$), mais aussi l'apparition d'un inverse pour certains éléments ($\bar{3}\times\bar{3}=\bar{1}$).

L'apparution de « diviseurs de zéro » est un fait nouveau donc un peu troublant. C'est un fait propre aux ensembles quotients $\mathbb{Z}/n\mathbb{Z}$. Ce fait simplifie grandement les calculs dans ces structures. Quant aux « quelques » éléments inversibles, leur caractérisation est à la base de beaucoup de résultats féconds d'arithmétique.

Définition 30. (Diviseurs de zéro) *Dans l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z}$*, un élément* $\bar{x}$ *est un diviseur de zéro s'il est différent* $\bar{0}$ *et s'il existe* $\bar{y}\neq\bar{0}$ *dans* $\mathbb{Z}/n\mathbb{Z}$ *tel que* $\bar{x}\times\bar{y}=\bar{0}$*.*

Définition 31. (Éléments inversibles) *Dans l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z}$*, un élément* $\bar{x}$ *est inversible s'il existe* $\bar{y}$ *dans* $\mathbb{Z}/n\mathbb{Z}$ *tel que* $\bar{x}\times\bar{y}=\bar{1}$*. L'ensemble des éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *se note* $(\mathbb{Z}/n\mathbb{Z})^{\times}$*.*

Proposition 32. (Groupe des éléments inversibles) *L'ensemble* $(\mathbb{Z}/n\mathbb{Z})^{\times}$ *des éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *est non vide, stable par multiplication et par passage à l'inverse.*

On dit que $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$ *est un* ***groupe*** *pour évoquer les propriétés précédentes.*

Démonstration. **Exercice 14.** □

Le théorème suivant est fondamental en arithmétique.

Théorème. (de Bézout) *Soient* $a, b\in\mathbb{Z}$*. Il existe* $(u, v)\in\mathbb{Z}^2$ *tel que* $\text{pgcd}(a, b)=ua+vb$*.*

Démonstration. **Exercice 15.** □

Remarque 33. Le couple $(u, v)\in\mathbb{Z}^2$ tel que $\text{pgcd}(a, b)=ua+vb$ n'est pas unique.

Proposition 34. (Caractérisation des diviseurs de zéro et des inversibles de $\mathbb{Z}/n\mathbb{Z}$)

1. *Dans l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z}=\{\bar{0}, \bar{1}, ..., \overline{(n-1)}\}$*, un élément* $\bar{x}$ *est diviseur de zéro si et seulement si* $x\neq 0$*,* $x\neq 1$ *et* x *divise* n*.*
2. *Dans l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{(n-1)}\}$*, un élément* $\bar{x}$ *est inversible si et seulement si* x *et* n *sont premier entre eux (i.e* $\text{pgdc}(x, n)=x\wedge n=1$*).*

Démonstration. **Exercice 16.** □

2.4 Division « entière » informatique et division euclidienne.

La plupart des langages de programmation utilisés en informatique disposent d'un type de données pour représenter ce que les informaticiens appellent les entiers signés (les entiers relatifs) et possèdent des opérateurs pour effectuer les calculs classiques sur ces nombres.

En C ou java, par exemple, le symbole / représente le quotient dans la « division entière » et le symbole % représente ce que les informaticiens appellent improprement le modulo (le reste dans leur « division entière »).

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

Pour des raisons pratiques de réalisation des micro-circuits des processeurs qui réalisent ces opérations, la « division entière » ne donne pas exactement le même résultat que la division euclidienne.

Considérons par exemple les 4 cas possibles de division euclidienne de a par b lorsque $|a|=29$ et $|b|=7$ (en n'oubliant pas que le reste d'une division euclidienne ne peut être que positif)

a	b	division euclidienne	q	r	a/b	$a\%b$
29	7	$29 = 4 \times 7 + 1$	4	1	4	1
29	-7	$29 = (-4) \times (-7) + 1$	-4	1	-4	1
-29	7	$-29 = (-5) \times 7 + 6$	-5	6	-4	-1
-29	-7	$-29 = 5 \times (-7) + 6$	5	6	4	-1

Autrement dit, mathématiquement, le quotient est positif lorsque les deux nombres ont le même signe et le reste est toujours positif, et, pour que le reste soit toujours positif, le quotient peut ne pas être le quotient des valeurs absolues.

Informatiquement, le « quotient » est positif lorsque les nombres ont le même signe, le « reste » a le signe du dividende, et la valeur absolue du « quotient » est toujours le quotient des valeurs absolues.

Dans les applications de calcul arithmétique, par exemple un calcul de PGCD, ce n'est pas gênant parce que les restes « informatiques » sont congrus aux restes mathématiques modulo la valeur absolue du diviseur, et qu'il ne s'agit alors que du choix d'un représentant de la classe concernée (addition et multiplication étant compatibles avec la congruence modulo n).

Mais il faut quand même savoir que l'on peut obtenir un « reste » négatif et prendre ses dispositions le cas échéant...

2.5 Arithmétique modulo 2^n dans les ordinateurs

Présentation générale. Les calculs sur les entiers, dans un ordinateur, se font dans $\mathbb{Z}/2^n\mathbb{Z}$, où n est le nombre de bits utilisés dans la représentation de ces nombres. Dans la plupart des microprocesseurs, les entiers sont représentés sur 32 bits, les calculs se font donc dans $\mathbb{Z}/2^{32}\mathbb{Z}$ (et qu'ils le soient sur 64 bits ne change rien au problème).

Disposer d'entiers signés ou d'entiers non signés est uniquement une question de choix du représentant dans les classes d'équivalence, mais la représentation physique est la même.

Comme il nous est difficile de représenter ici la liste complète de tous ces entiers, nous allons illustrer ce propos en supposant que les entiers sont représentés sur 4 bits.

Illustration dans le cas de 4 bits. Pour des mots de 4 bits, il y a alors 16 entiers représentables : (a.s.= arithmétique signée, a.n.s. = arithmétique non signée)

code binaire		a.s.	a.n.s.
0000	interprété par	0	0
0001	interprété par	1	1
0010	interprété par	2	2
0011	interprété par	3	3
0100	interprété par	4	4
0101	interprété par	5	5
0110	interprété par	6	6
0111	interprété par	7	7
1000	interprété par	8	-8
1001	interprété par	9	-7
1010	interprété par	10	-6
1011	interprété par	11	-5
1100	interprété par	12	-4
1101	interprété par	13	-3
1110	interprété par	14	-2
1111	interprété par	15	-1

Pourquoi ce choix ? Pourquoi ne pas avoir, en a.s., représenté les entiers dans l'ordre croissant de 0000 (-8) à 1111 (7) ?

- Tout simplement pour des raisons d'efficacité : 0 doit toujours être représenté par le code « nul » 0000.

- Ensuite, il faut pouvoir comparer efficacement ces codes entre eux, ce qui explique que 0 doit être suivi de 1, arithmétique signée ou pas.

Ces principes ont ainsi conduit à placer les codes interprétés comme entiers négatifs après ceux qui représentent les entiers positifs.

Par ailleurs, on s'aperçoit que, de cette manière, les codes des entiers négatifs commencent tous par 1. On parle improprement de « bit de signe » : s'il s'agissait d'un véritable bit de signe, le code 1001 devrait être celui de -1, or c'est celui de -7. Mais il n'en reste pas moins que tous les entiers négatifs commencent par 1).

Ainsi, il est facile de déduire la comparaison signée de la comparaison non signée : les codes qui commencent par 1 sont « plus petits » que ceux qui commencent par 0, et, s'ils commencent par le même bit, c'est la comparaison non signée qui peut être utilisée.

Mais il y a quand même deux instructions assembleur distinctes pour la comparaison signée et pour la comparaison non signée.

3 Algorithme d'Euclide et applications

3.1 PGCD de deux entiers relatifs

On a vu plus haut la justification de l'existence du pgcd de deux nombres strictement positifs par comparaison de leurs décompositions en facteurs premiers. Par définition, le pgcd de a non nul avec 0 est a (défintion raisonnable, car 0 est divisible par tout entier non nul, donc par a, qui l'est aussi par a) et enfin le pgcd de 0 et de 0 n'est pas défini. Il est possible de considérer des nombres négatifs (bien que ce soit sans grand intérêt dans les applications pratiques), mais le pgcd est celui des valeurs absolues.

L'algorithme consistant à comparer les décompositions en facteurs premiers n'est pas efficace, la découverte de diviseurs de nombres très grands est un problème difficile dont nous reparlerons plus loin.

3.2 Algorithme d'Euclide

On se limite ici au cas de deux entiers a et b strictement positifs.

Théorème 35. (Algorithme d'Euclide) *Soit (r_n) la séquence définit par $r_0 = a$, $r_1 = b$ et le procédé récursif suivant :*

1. $r_2 = \text{rem}\,(r_0, r_1)$ *où* $\text{rem}(r_0, r_1)$ *est le reste de la division euclidienne de* r_0 *par* r_1,
2. *si* $r_2 \neq 0$, $r_3 = \text{rem}(r_1, r_2)$,
3. *si* $r_3 \neq 0$, $r_4 = \text{rem}(r_2, r_3)$,
   $\vdots$
4. $r_k \neq 0$, $r_{k+1} = \text{rem}(r_{k-1}, r_k)$,

Soit n_0 l'ordre du premier reste nul rencontré durant le processus récursif décrit. Alors r_{n_0-1} est le pgcd de a et b.

Démonstration. **Exercice 17.** □

Remarque 36. L'algorithme décrit dans le Théorème 35 permet donc d'obtenir le PGCD de deux nombres sans connaître leurs décompositions en facteurs premiers.