CNAM MULHOUSE .

Technicien Développeur Année 1.

Outils mathématiques

Cours Michel GOZE

Chapitre 3

Congruence. Bases et Codages

1. La relation de congruence

1.1. **Définition de la congruence modulo p.** Soit p un entier positif donné.

Définition 1. *Soient m et n deux entiers. n dit que m est congru à n modulo p et on écrit*

$$m \equiv n \pmod{p}$$

ou parfois pour raccourcir l'écriture

$$m \equiv n \ [p]$$

si p divise la différence $m - n$.

Ceci est aussi équivalent à dire que m et n ont les mêmes restes dans la division euclidienne par p. Cette relation est appelée la relation de congruence modulo p.

Exemples

(1) $18 \equiv 13 \pmod{5}$

(2) $m = 2k \equiv 0 \pmod{2}$, où $k \in \mathbb{Z}$.

(3) $m = 2k + 1 \equiv 1 \pmod{2}$, où $k \in \mathbb{Z}$.

Théorème 1. *La relation de congruence modulo p est une relation d'équivalence, c'est-à-dire*

(1) Elle est Réflexive : $m \equiv m \pmod{p}$

(2) Elle est Symétrique : $m \equiv n \pmod{p}$ implique $n \equiv m \pmod{p}$

(3) Elle est Transitive : Si $m \equiv n \pmod{p}$ et $n \equiv r \pmod{p}$ alors $m \equiv r \pmod{p}$.

Démonstration. Elle est en effet

(1) Réflexive car $m - m$ a pour reste 0 dans la division par p.

(2) Symétrique car si $m - n$ a pour reste 0 il en est aussi de même de $n - m$ dans la division par p,

(3) Transitive. En effet si m_1 est congru à m_2 modulo p et m_2 congru à m_3 modulo p, alors $m_1 - m_2$ est divisible par p, c'est-à-dire $m_1 - m_2 = kp$, $m_2 - m_3$ est aussi divisible par p, soit $m_2 - m_3 = k_2 p$. Ainsi

$$m_1 - m_3 = m_1 - m_2 + m_2 - m_3 = kp + k_1 p = (k + k_1)p$$

et $m - m_2$ est aussi divisible par p soit m_1 congru à m_3 modulo p, ce qui montre la transitivité. La relation de congruence modulo p est donc Réflexive, Symétrique et Transitive. C'est une relation d'équivalence.

1.2. **Addition,soustraction et multiplication de nombres congruents.** Nous allons regarder le comportement de cette relation par rapport aux opérations arithmétiques ordinaires.

Proposition 1. *Soit p un entier positif donné et soient m_1, m_2, n_1, n_2 des entiers tels que*

$$m_1 \equiv m_2 \pmod{p}, \quad n_1 \equiv n_2 \pmod{p}.$$

Alors

(1) $m_1 + n_1 \equiv m_2 + n_2 \pmod{p}$,

(2) $m_1 - n_1 \equiv m_2 - n_2 \pmod{p}$,

(3) $m_1 n_1 \equiv m_2 n_2 \pmod{p}$

Démonstration. La démonstration est facile et laissée au lecteur. Il suffit de se servir des hypothèses :

$$m_1 - m_2 = k_1 p, \quad n_1 - n_2 = k_2 p.$$

La troisième propriété est un peu plus délicate à établir. On écrit

$$m_1 n_1 - m_2 n_2 = m_1 n_1 - m_1 n_2 + m_1 n_2 - m_2 n_2 = m_1(n_1 - n_2) + (m_1 - m_2)n_2$$

ce qui permet de conclure.

Par contre, pour la division les choses sont moins simples. Nous y reviendrons en fin de cours dans l'étude de certaines structures algébriques.

1.3. **L'ensemble des classes d'équivalence.** Considérons la relation d'équivalence modulo p. Soit m un entier. Sa classe d'équivalence est par définition le sous-ensemble de $\mathbb{Z}$, noté $\mathrm{cl}(m)$ et défini comme suit :

$$\mathrm{cl}(m) = \{n \in \mathbb{Z},\ n \equiv m \pmod{p}\}.$$

Proposition 2. *Pour p entier positif donné, il existe p classes d'équivalence pour la relation de congruence modulo p, à savoir*

$$\mathrm{cl}(0), \mathrm{cl}(1) \cdots, \mathrm{cl}(p-2), \mathrm{cl}(p-1).$$

Démonstration. En effet, si r est le reste de la division de m par p, alors $0 \leq r < p$ et $m \equiv r \pmod{p}$. Comme les restes de la division par p sont les entiers positifs compris entre 0 et $p-1$, on en déduit qu'il y a au plus p classes d'équivalence, celles décrites dans la proposition. Il reste à montrer que ces classes forment une partition de $\mathbb{Z}$. Il est clair que la réunion de ces classes est l'ensemble $\mathbb{Z}$. Montrons que leurs intersections sont vides. Si $n \in \mathrm{cl}(r_1)$ et $n \in \mathrm{cl}(r_2)$ alors le reste de la division de n par p est r_1 et r_2, ce qui implique $r_1 = r_2$ et donc $\mathrm{cl}(r_1) = \mathrm{cl}(r_2)$.

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble quotient associé à cette relation, c'est-à-dire l'ensemble des classes d'équivalence. On en déduit

$$\mathbb{Z}/p\mathbb{Z} = \{\mathrm{cl}(0), \mathrm{cl}(1) \cdots, \mathrm{cl}(p-2), \mathrm{cl}(p-1)\}.$$

Par soucis de simplification d'écriture, nous adopterons l'écriture suivante

$$\mathrm{cl}(m) = \overline{m}^{(p)}$$

ou si la précision de p est superflue, car sous-entendue

$$\mathrm{cl}(m) = \overline{m}.$$

Les opérations sur les classes s'écrivent alors

$$\overline{m} + \overline{n} = \overline{m+n}, \quad \overline{m} \cdot \overline{n} = \overline{mn}$$

mais en prenant garde qu'il s'agit toujours de la congruence modulo le même entier.

Exemples.

(1) $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$.

(2) $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

(3) $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Comme ces ensembles sont finis et munis de deux opérations $+$ et $\times$, nous pouvons dresser les tables de ces opérations.

Exemples.

(1) Dans $\mathbb{Z}/2\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

,

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

(2) Dans $\mathbb{Z}/3\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

,

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(3) Dans $\mathbb{Z}/4\mathbb{Z}$ les tables d'addition et de multiplication s'écrivent

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

,

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

Nous étudierons plus en détail les propriétés de ces opérations dans le dernier chapitre consacré aux structures algébriques.

2. Applications : les preuves par 3, 5 et 9

2.1. **Quelques calculs avec la congruence.** Nous avons vu, ci-dessus, la relation : soit p un entier positif donné et soient m_1, m_2, n_1, n_2 des entiers tels que $m_1 \equiv m_2 \pmod{p}$, $n_1 \equiv n_2 \pmod{p}$, alors

$$m_1 n_1 \equiv m_2 n_2 \pmod{p}.$$

Nous en déduisons immédiatement

Proposition 3. *Soit p un entier positif donné et soient m_1, m_2 des entiers tels que $m_1 \equiv m_2 \pmod{p}$, alors pour tout $k \in \mathbb{N}$*

$$m_1^k \equiv m_2^k \pmod{p}.$$

Exemples.

(1) Modulo 3 : Nous savons que $10 \equiv 1 \pmod{3}$. Nous en déduisons que pour tout $k \in \mathbb{N}$,

$$10^k \equiv 1 \pmod{3}$$

et aussi

$$10^k + 2 \equiv 1 + 2 \pmod{3}.$$

Mais comme $2 + 1 = 3 \equiv 0 \pmod{3}$, nous obtenons, pour tout $k \in \mathbb{N}$,

$$10^k + 2 \equiv 0 \pmod{3}$$

et donc $10^k + 2$ est divisible par 3.

(2) Modulo 7 : Nous voulons simplifier l'expression $93^{1002} + 93^{1001} + 93^{1000} \pmod{7}$. Considérons l'entier 93. On vérifie sans peine que $93 \equiv 2 \pmod{7}$. Nous en déduisons que pour tout entier k, $93^k \equiv 2^k \pmod{7}$. Mais $2^3 \equiv 1 \pmod{7}$. Ceci implique

$$2^{999} \equiv 1 \pmod{7},\ 2^{1000} \equiv 2 \pmod{7},\ 2^{1001} \equiv 4 \pmod{7},\ 2^{1002} \equiv 1 \pmod{7}.$$

Ainsi

$$3^{1002} + 93^{1001} + 93^{1000} \equiv (2 + 4 + 1) \equiv 0 (\text{mod } 7).$$

2.2. **La preuve par 3 ou par 9.** Considérons un nombre entier n écrit sous sa forme décimale :

$$n = a_1 a_2 \cdot a_p$$

avec $a_i \in \{0, 1, 2, \cdots, 9\}$. Par exemple $n = 5432$, alors $a_1 = 5, a_2 = 4, a_3 = 3, a_4 = 2$. Cette écriture est équivalente à

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p.$$

Par exemple $5432 = 5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2$. Mais nous avons $10 \equiv 1 (\text{mod } 3), 10^2 \equiv 1 (\text{mod } 3)$ et donc plus généralement, pour tout $k \in \mathbb{N}$:

$$10^k \equiv 1 (\text{mod } 3).$$

Ainsi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv a_1 + a_2 + \cdots + a_p \pmod{3}.$$

De même nous avons $10 \equiv 1 \pmod{9}$ et donc pour tout entier k, $10^k \equiv 1 \pmod{9}$. Nous aurons donc aussi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv a_1 + a_2 + \cdots + a_p \pmod{9}.$$

On en déduit la règle de divisibilité :

Proposition 4. *(1) Un nombre entier n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.*

(2) Un nombre entier n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

2.3. **La preuve par 11.** D'après ce que nous venons de voir, les critères de divisibilité par un entier p repose sur l'étude de $10^k \pmod p$. Ici $p = 11$ et $10 \equiv -1 \pmod{11}, 10^2 \equiv 1 \pmod{11}$, $10^3 \equiv -1 \pmod{11}$, ce qui donne en général

$$10^{2k} \equiv 1 \pmod{11},\ 10^{2k+1} \equiv -1 \pmod{11}.$$

Ainsi

$$n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \cdots + a_{p-1} \cdot 10 + a_p \equiv (-1)^{p-1}a_1 + (-1)^{p-2}a_2 - a_{p-1} + a_p.$$

Proposition 5. *Un nombre est divisible par 11 lorsque la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de 11.*

Prenons par exemple $n = 5432$. Nous avons

$$5432 \equiv -5 + 4 - 3 + 2 = -2 = 9 \ (\mod 11).$$

De meme $25432 \equiv 2 - 5 + 4 - 3 + 2 = 0 \ (\mod 11)$ et donc ce nombre est divisible par 11.

2.4. **Quelques autres règles de divisibilité.** On pourra, à titre d'exercices, démontrer de manière analogue d'autres règles de divisibilté

Proposition 6. *(1) Un nombre est divisible par 4 lorsque les deux chiffres de droite forment un nombre multiple de 4.*

(2) Un nombre est divisible par 5 lorsque le chiffre des unités est 0 ou 5.

(3) Un nombre est divisible par 8 lorsque les trois chiffres de droite forment un nombre multiple de 8.

Il existe également un critère de divisibilité par 7, mais cela commence à devenir peu simple à utiliser. On séparer ce nombre par tranches de trosi chiffres en partant des unités et d'insérer alternativement des $-$ et des $+$ entre les tranches. On effectue l'opération ainsi écrite et ce résultat est divisible par 7 si et seulement le nombre de départ l'est.

3. Systèmes de numération décimal et binaire

3.1. **Le système décimal.** La numération est un moyen de représenter un nombre à l'aide de symboles. Cette manière a varié au cours des temps. Le système en vigueur aujourd'hui, dans la vie courante, est basé sur dix symboles, $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. On l'appelle donc le système décimal. Dans les paragraphes suivants, nous présenterons des systèmes utilisés de nos jours mais dans des domaines orientés vers l'informatique, le système binaire qui repose sur 2 symboles, le 0 et le 1, et le système bibinaire qui repose sur seize symboles (il faudra donc leur trouver une calligraphie).

Considérons donc un nombre entier N positif. Il s'écrit, en écriture décimale

$$N = a_p 10^p + a_{p-1}10^{p-1} + \cdots + a_1 10 + a_0$$

a_0 étant le chiffre des unités, a_1 celui des dizaines, etc (voir le cours de CM1). Les "chiffres" $a_0, a_1, \cdots, a_p$ appartient à $\{0, 1, \cdots, 9\}$ et sont parfois appelés les digits (langage informatique).

Cette écriture s'étend également aux nombres décimaux (cf cours CM2), l'écriture sera alors donnée de la façon suivante

$$N = \sum_{i=-m}^{i=p} a_i 10^i$$

où m et p sont des entiers positifs ou nuls.

Dans le système binaire, qui est le système fondamental en informatique, seuls deux symboles sont utilisés communément appelés en langage informatique bits. Ces symboles sont notés, car aucune confusion n'est possible avec les symboles qui ont la même calligraphie dans le système décimal, 0 et 1. L'écriture d'un nombre dans ce système est basée sur la relation suivante : tout nombre entier s'écrit de manière unique sous la forme

$$N = u_p 2^p + u_{p-1} 2^{p-1} + \cdots + u_1 2 + u_0$$

où les nombres entiers u_i appartiennent à $\{0, 1\}$. Si dans l'écriture décimale on convient d'écrire un nombre de droite à gauche dans l'ordre unité, dizaine , centaine etc, il en sera de même en écriture binaire. On écrira le nombre N sous la forme

$$\overline{u_p u_{p-1} \cdots u_1 u_0}^{(2)}.$$

Si aucune confusion n'est possible, s'il est précisé auparavant que le système de numération utilisé est le binaire, alors dans ce cas, nous simplifierons l'écriture en écrivant

$$u_p u_{p-1} \cdots u_1 u_0.$$

Ainsi la suite des nombres ordonnée dans le système binaire commence ainsi

$$\begin{cases} 0 \\ 1 \\ 10 \\ 11 \\ 100 \\ 101 \\ 110 \\ 111 \\ 1000 \\ 1001 \\ \cdots \end{cases}$$

Chacun de ces nombres est représenté dans le système décimal par $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \cdots$.

Comment passer du système décimal au système binaire ? Cette opération s'appelle le codage. Une méthode algorithmique efficace, basée sur l'écriture $N = u_p 2^p + u_{p-1} 2^{p-1} + \cdots + u_1 2 + u_0$ du nombre donné et utilisant la division euclidienne par 2. On écrit la suite suivante de division euclidienne

$$\begin{aligned} N &= 2N_1 + \mathbf{r_0} \\ N_1 &= 2N_2 + \mathbf{r_1} \\ N_2 &= 2N_3 + \mathbf{r_2} \\ &\cdots \\ N_{p-1} &= 2N_p + \mathbf{r_{p-1}} \\ N_p &= 2 \cdot 0 + \mathbf{r_p} \end{aligned}$$

L'écriture du nombre N en base 2 (ou écriture binaire) est alors

$$\mathbf{r_p r_{p-1} \cdots r_2 r_1 r_0}.$$

(On fera très attention au fait que le premier reste trouvé est celui des "unités", le deuxième celui des "deuxaines",...) Il est clair que cet algorithme s'arrête lorsque l'un des quotients est plus petit que 2. Un exercice intéressant est de programmer cet algorithme sur PYTHON.

Exemple. On veut coder en binaire le nombre 11. On a

$$\begin{aligned} 11 &= 2 \times 5 + \mathbf{1} \\ 5 &= 2 \times 2 + \mathbf{1} \\ 2 &= 2 \times 1 + \mathbf{0} \\ 1 &= 2 \times 0 + \mathbf{1} \end{aligned}$$

et donc 11 s'écrit en binaire 1011.

Comment passer du système binaire au système décimal ? Cette opération s'appelle le décodage. Elle est particulièrement simple. Il suffit d'utiliser la décomposition en bits. Si on considère un nombre $N = \overline{u_p i_{p-1} \cdots u_1 u_0}^{(2)}$ écrit en binaire, il s'écrit en décimal $N = u_p 2^p + u_{p-1} 2^{p-1} + \cdots + u_1 2 + u_0$. Par exemple, considérons $N = \overline{1011}^{(2)}$, alors

$$N = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 8 + 2 + 1 = 11.$$

4. Système de numération en base b

Considérons un entier $b \geq 2$. Cet entier sera appelé la base du système de numération. Pour le système décimal, $b = 10$, pour le système binaire, $b = 2$.

4.1. Ecriture d'un nombre en base b.

Théorème 2. *Tout entier N positif s'écrit de manière unique sous la forme*

$$N = a_p b^p + a_{p-1} b^{p-1} + \cdots + a_1 b + a_0$$

où les a_i sont des entiers vérifiant $0 \leq a_i \leq b - 1$.

Démonstration. L'unicité se prouve assez facilement : supposés que l'on ait deux décompositions

$$N = a_p b^p + a_{p-1} b^{p-1} + \cdots + a_1 b + a_0 = b(a_p b^{p-1} + a_{p-1} b^{p-2} + \cdots + a_1) + a_0.$$

Ainsi a_0 qui vérifie $0 \leq a_0 \leq b - 1$ est le reste de a division euclidienne de N par b. Il est donc unique. On considère ensuite l'entier $(N - a_0)b^{-1}$ et on réitère le raisonnement que nous avons fait pour a_0. Reste à prouver l'existence de cette décomposition. Cette preuve nous donne en fait la procédure du codage d'un nombre en base b. Nous la développons ci-dessous.

Comment passer du système décimal au système en base b ? Cette opération s'appelle toujours le codage. La méthode algorithmique efficace, identique à celle présentée pour $b = 2$

est basée sur l'écriture $N = u_p b^p + u_{p-1} b^{p-1} + \cdots + u_1 b + u_0$ du nombre donné et utilisant la division euclidienne par b. On écrit la suite suivante de division euclidienne

$$\begin{aligned} N &= bN_1 + \mathbf{r_0} \\ N_1 &= bN_2 + \mathbf{r_1} \\ N_2 &= bN_3 + \mathbf{r_2} \\ &\cdots \\ N_{p-1} &= bN_p + \mathbf{r_{p-1}} \\ N_p &= b \cdot 0 + \mathbf{r_p} \end{aligned}$$

L'écriture du nombre N en base b est alors

$$\overline{r_p r_{p-1} \cdots r_2 r_1 r_0}^{(b)}.$$

Exemple. Ecrire en base 9 le nombre 1237. Bien entendu 1237 est l'écriture décimale, ce que nous conviendrons lorsqu'aucune base n'est précisée. On a

$$\begin{aligned} 1237 &= 9 \times 137 + \mathbf{4} \\ 137 &= 9 \times 15 + \mathbf{2} \\ 15 &= 9 \times 1 + \mathbf{6} \\ 1 &= 9 \times 0 + \mathbf{1} \end{aligned}$$

Ainsi 1237 s'écrit en base 9 :

$$\overline{1624}^{(9)}.$$

Notons que le décodage, c'est-à-dire le passage à l'écriture décimale, se fait, comme en base 2 en utilisant le développement en puissance de b.

4.2. **Le système octal.** Il correspond au système numérique en base 8. On peut passer facilement du système binaire au système octal (en fait on sait passer facilement du système binaire à un système de base 2^k). La règle générale de conversion est la suivante :

(1) En allant de droite à gauche , on scinde l'expression binaire en paquets de 3 chiffres (3 est l'exposant de 2 dans $b = 8 = 2^3$).

(2) Comme en base 2, le nombre 7 s'écrit $\overline{111}^{(2)}$, un paquet de 3 chiffre composés de 0 et de 1 représente un nombre plus petit que 7.

(3) On remplace chacun des groupes, correspondant à l'écriture en base 2 d'un nombre plus petit ou égal à 7 par ce nombre.

Exemple. Soit le nombre qui s'écrit en base 2

$$\overline{100110110101}^{(2)}.$$

Cherchons son expression en base 8 en suivant les étapes suivantes

$$\begin{aligned} &\overline{100110110101}^{(2)} \\ &100; 110; 110; 101 \\ &4; 6; 6; 5 \end{aligned}$$

l'écriture cherchée est donc

$$\overline{4665}^{(8)}.$$

4.3. **Cas où la base b est plus grande que 10 : un exemple, le système bibibinaire.** Lorsque $b \geq 10$, l'écriture d'un nombre sous la forme

$$N = a_p b^p + a_{p-1} b^{p-1} + \cdots + a_1 b + a_0$$

fait apparaître des composantes a_i qui sont inférieures ou égales à $b-1$. Mais nous ne pouvons plus utiliser comme composantes les nombres $10, 11, 12, \cdots, b-1$ car ils représentent déjà des codes en système décimal. Il est alors d'usage d'utiliser des lettres majuscules, $A, B, C, \cdots,$. Comme nous pouvons supposer que b n'est pas trop grand, l'alphabet devrait suffire pour satisfaire ce besoin.

Un exemple intéressant, utilisé en informatique, est le système hexadécimal correspondant à $b = 16$. Le symboles de base sont alors

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

Il est largement utilisé en informatique car, comme nous l'avons vu ci-dessus, il est très facile de passer du système binaire au système hexadécimal. En effet $16 = 2^4$, on découpe alors le nombre écrit en base 2 en paquet de 4 en partant de la droite et on remplace chaque paquet par le nombre correspondant en écriture décimale qui sera nécessairement un nombre inférieur ou égal à 15, en prenant soin de remplacer 10 par A, 11 par B, 12 par C, 13 par D, 14 par E et 15 par F. Par exemple le nombre qui s'écrit en base 2

$$\overline{100110110101}^{(2)}$$

s'écrira, en suivant la règle de conversion

$$\begin{array}{l} \overline{100110110101}^{(2)} \\ 1001; 1011; 0101 \\ 9; 11; 5 \end{array}$$

l'écriture cherchée est donc

$$\overline{9B5}^{(16)}.$$

Un peu d'histoire. Le système hexadécimal a été étudié pour la première fois par le chanteur Boby Lapointe dans sa thèse de Doctorat soutenue à l'Université de Montpellier en 1968. Pour situer un peu ce chanteur, voici le refrain d'une de ses célèbres chanson, intitulée Ta Katie t'a quitté :

Tic-tac tic-tac

Ta Katie t'a quitté

Tic-tac tic-tac

Ta Katie t'a quitté

Tic-tac tic-tac

T'es cocu, qu'attends-tu ?

Cuite-toi, t'es cocu

T'as qu'à, t'as qu'à t' cuiter

Et quitter ton quartier

Ta tactique était toc

Ta tactique était toc

Revenons au système hexadécimal de Boby Lapointe. Il en a décrit toute l'arithmétique et montrer son importance comme outil numérique. Il ne l'appelait pas hexadécimal mais bibibinaire car $16 = 2^{2^2}$. Il avait utilisé 16 symboles pour décrire les composantes d'un nombre à la place de $0, 1, \cdots, F$ utilisés de nos jours. Pour pouvoir lire ces symboles, comme on lit *zéro* pour 0, un pour 1, etc, il utilisait 4 voyelles et 4 consonnes. Plus précisément la prononciations des symboles $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ était dans l'ordre

HO, HA, HE, HI, BO, BA, BE, BI, KO, KA, KE, KI, DO, DA, DE, DI.

Par exemple le nombre 2000 se lit en bibibinaire $BIDAHO$.

4.4. **Retour au binaire. Code correcteur.** Le but d'un réseau est de transmettre des informations d'un ordinateur à un autre. Passons sur les divers moyens techniques pour assurer cette transmission, et restons sur l'échange de données qui est basée sur un codage de l'information. Supposons que ce codage soit supporté par un langage binaire. Une étape importante et fondamentale au cours de ces échanges est celle du contrôle des erreurs : est-ce qu'une information codée émise est correctement interprétée par le destinataire. Les erreurs doivent impérativement être détectées dès leur apparition. Par exemple le mot envoyé est codé en binaire par 10101101. Le destinataire reçoit ce code est doit s'assurer que c'est bien le code envoyé par l'expéditeur.

Première méthode : Introduction d'un bit de parité. On rajoute au mot binaire envoyé un bit supplémentaire On choisit par exemple le 1 si la somme des 1 du mots codés est impaire et 0 sinon. A la réception, on vérifie en lisant le bit de contrôle, situé en fin de mot, que la parité est bien respectée. Il est clair que ce test peut être lui aussi erroné mais il est simple à mettre en place et renseigne si le test est faux (un peu comme la règle de 3 pour la multiplication). Il ne renseigne pas sur la position dans le mot de l'erreur.

Deuxième méthode. Introduction d'un mot de parité. Cette méthode permet de localiser presque à coup sûr l'erreur. Supposons par exemple que l'on veuille tester un nombre binaire comprenant 4 bits, c'est-à-dire $\overline{a_1a_2a_3a_4}^{(2)}$. On rajoutera à ce code 3 bits supplémentaires de parité, le premier pour le code $\overline{a_1a_2a_3}^{(2)}$, le deuxième pour $\overline{a_1a_2a_4}^{(2)}$ le troisième pour $\overline{a_1a_3a_4}^{(2)}$. Cela est suffisantt pour localiser une erreur chez le destinataire.

5. Arithmétique en binaire

5.1. **L'addition.** La technique d'addition est la même que celle en base 10, on reporte les retenues sur la colonne de gauche immédiate, ou si cette retenue a plusieurs bits, sur les colonnes de gauche en partant de celle qui jouxte. Par exemple

$$\begin{array}{cccccc} & 1 & 0 & 1 & 1 \\ + & 1 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 0 \end{array}$$

5.2. **La multiplication.** Pour cette opération aussi la technique est le même, avec un gros avantage, les seules tables de multiplication à connaître sont celles de 0 et de 1 (vieux traumatisme du CE1-CE2). Par exemple

$$\begin{array}{cccccccc} & & & 1 & 0 & 1 & 0 \\ & & \times & 1 & 1 & 0 & 0 \\ \hline & & & 0 & 0 & 0 & 0 \\ & & 0 & 0 & 0 & 0 & \\ & 1 & 0 & 1 & 0 & & \\ 1 & 0 & 1 & 0 & & & \\ \hline 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}$$

6. L'exponentiation modulaire

Etant donné un entier n "grand", on souhaiterait calculer le reste modulo n d'une puissance a^p d'un entier donné. Nous donnerons une application de ce problème concernant le cryptage.

6.1. **Calculer le reste modulo n de a^p, avec n grand.** L'exponentiation modulaire (ou puissance modulo) est le résultat du calcul a^p modulo n. Elle est utilisée en informatique et en cryptographie. Par exemple, quel est le reste modulo 56 de 12^{34} ?.

Première méthode : la méthode naïve. On calcule le reste de a modulo n. Soit r_1 ce reste. On calcule ensuite le reste de $a \cdot r_1$ modulo n. Soit r_2 ce reste. Puis le reste de $a \cdot r_2$. On continue ainsi b fois, et le dernier reste obtenu sera le résultat cherché. Dans notre exemple, nous aurons

$$12 = 12\ (56), 144 = 32\ (56), 12 \times 32 = 384 = 48\ (56), 48 \times 12 = 576 = 16\ (56) = \cdots$$

Ce calcul est long. Il nécessite $b = 34$ opérations.

Deuxième méthode. On décompose l'exposant b en somme de puissance de 2. Rappelons ces puissances :

$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64, 2^7 = 128, 2^8 = 256, 2^9 = 512, 2^{10} = 1024, \cdots$

On aura donc

$$b = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_r}$$

avec $k_1 > k_2 \cdots > k_r \geq 0$. On en déduit

$$a^b = a^{2^{k_1}+2^{k_2}+\cdots+2^{k_r}} = a^{2^{k_1}} \cdot a^{2^{k_2}} \cdots a^{2^{k_r}}.$$

Dans notre exemple, la décomposition de $b = 34$ en somme de puissance de 2 est

$$34 = 32 + 2 = 2^5 + 2^1.$$

Ainsi

$$12^{34} = 12^{2^5} \cdot 12^2.$$

Revenons au cas général. La décomposition de b en somme de puissance de 2 ramène notre calcul à trouver les restes modulo n de a élevé à une puissance de 2. On va donc calculer

(1) le reste r_1 modulo n de a
(2) le reste r_2 modulo n de $r_1 \times a$
(3) le reste r_3 modulo n de $r_2 \times a$
(4) $\cdots$
(5) enfin le reste r_{k_1} modulo n de $r_{k_1-1} \times a$.

Notons que certaine étapes peuvent être éviter suivant les valeurs des exposants.

Reprenons notre exemple

(1) $a = 12 \equiv 12$ modulo 56
(2) $r_1 \times 12 = 12^2 \equiv 32$ modulo 56 ceci correspondant à a^2
(3) $r_2 \times 12 = 384 \equiv 48$ modulo 56 ceci correspondant à a^3
(4) $r_3 \times 12 = 576 \equiv 16$ modulo 56 ceci correspondant à a^4
(5) $r_4 \times a = 192 \equiv 24$ modulo 56
(6) $r_5 = 16$.

Ainsi

$$12^{34} = 12^{2^5} \cdot 12^2 = 24 \times 32 \equiv 40 \text{ modulo } 56.$$

Ici on aurait pu se limiter aux seules opérations

(1) $a = 12 \equiv 12$ modulo 56
(2) $r_1 \times 12 = 12^2 \equiv 32$ modulo 56 ceci correspondant à a^2
(3) $r_2^2 = 1024 \equiv 16$ modulo 56 ceci correspondant à a^4
(4) $16 \times 12 = 192 \equiv 24$ modulo 56
(5) $r_5 = 16$.

6.2. **Application : le système de codage R.S.A.** Le système R.S.A est un système de codage basé sur deux clés publiques (c'est-à-dire connues par l'émetteur du message codé) et ces clés publiques appartiennent au receveur. Par exemple, l'émetteur du message voulant envoyer son message à un receveur précis trouvera ces clés dans un site public . Comment je constitue mes clés publiques personnelles :

(1) Je me donne deux nombres premiers p et q grands (on en connaît beaucoup) mais ces deux nombres je les garde secrets.
(2) Je fais le produits $n = pq$ et le produit $m = (p-1)(q-1)$.
(3) Je considère un entier e premier avec m

Les clés publiques sont n et e.

Considérons un message M que nous devons coder (M est un message chiffré, par exemple un code PIN). Nous voulons l'envoyer à un destinataire. Je vais rechercher sur un annuaire public les clés personnelles de ce destinataire. Soient n et e ces clés.

On considère maintenant le code chiffré

$$C \equiv M^e \bmod n.$$

A la reception, il faudra décoder C mais le receveur connait n, p, q, m, e. Soit d tel que

$$ed \equiv 1 \bmod m.$$

Alors

$$M \equiv C^d \bmod n.$$

Ce problème de déchiffrement se traite par l'exponentiation modulaire.

Remarque. Pour éviter toute tentative de pirater ce code, au lieu de coder directement m, on découpe M en paquets égaux de chiffres (plus grand que 2) et on code chaque paquets.

Exemple. Nicolas veut envoyer à Paul le message MATHS pour lui rappeler l'importance de ce cours. Il commence à l'écrire numériquement par exemple en utilisant la place des lettres dans l'alphabet. Ce mot devient

$$13\ 1\ 20\ 8\ 19.$$

On découpe ce nombre par paquets de 3 :

$$013\ 120\ 819.$$

Nicolas va chercher dans l'annuaire les clés de Paul. Il trouve $n = 5141$ et $e = 7$. En fait, en secret Paul avait choisit $p = 53, q = 97$ et donc $n = 5141, m = 4992$ et $e = 7$ est premier avec 4992. Nicolas va donc calculer

$$C_1 \equiv 013^7 \bmod 5141,\ C_2 = 120^7 \bmod 5141,\ C_3 = 819^7 \bmod 5141.$$

La méthode de l'exponentiation modulaire nous donne

$$C_1 = 2646,\ C_2 = \ C_3 = .$$

Paul doit décoder. Pour cela il utilise sa clé secrète d qui est donnée par $ed = \equiv 1 \bmod m$ soit comme $e = 7$ et $m = 5140 \times 4992$

EXERCICES

Exercice 1. Déterminer les congruences suivantes :

(1) Modulo 5 des nombres suivants : 12; 45; 87; 12; 104

(2) Modulo 7 des nombres suivants : 14; 85; 24; 46

(3) Modulo 8 des nombres suivants : 12; 204; 36; 48.

Exercice 2.

(1) Démontrer que $115 \equiv 27 \pmod{11}$

(2) Trouver un entier naturel n inférieur à 100 qui vérifie : $n \equiv 27 \pmod{11}$ et $n \equiv 4 \pmod{7}$.

(3) Combien d'entiers naturels inférieurs à 1000 sont congrus à 27 modulo 11 ?

Exercice 3. . Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.

(1) Vérifier que $8^7 \equiv 2 \pmod{55}$. En déduire le reste dans la division euclidienne par 55 du 8^{21}

(2) Vérifier que $8^2 \equiv 9 \pmod{55}$. En déduire le reste dans la division euclidienne par 55 de 8^{23}.

Exercice 4. Résoudre le système de congruence

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

Exercice 5. Résoudre le système de congruence

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{6} \end{cases}$$

En déduire la solution de l'énigme du pâtissier et de ses gâteaux.

Exercice 6.

(1) Montrer que pour tout n entier naturel, $5n^3 + n$ est divisible par 6.

(2) Montrer que si n n'est pas un multiple de 7 , alors $n^6 - 1$ est un multiple de 7.

(3) Montrer que pour tout entier naturel n , $n(n^2 + 5)$ est divisible par 6.

Exercice 7. Passage d'une base quelconque vers la base dix. Donner la valeur en base dix des nombres suivants.

(1) $(110101001)^{(2)}$.

(2) $(110101001)^{(3)}$.

Exercice 8. Effectuer chacune des additions suivantes de deux façons différentes : l'une en passant par la base dix et l'autre en posant l'addition et en calculant directement dans la base précisée.

(1) $(101101)^{(2)} + (111)^{(2)}$.

(2) $(2054)^{(7)} + (156)^{(7)}$.

Exercice 9. Sur le codage RSA. Rappelons le principe : Le système R.S.A est un système de codage basé sur deux clés publiques. Comment je constitue mes clés publiques personnelles :

— Je me donne deux nombres premiers p et q grands (on en connaît beaucoup) mais ces deux nombres je les garde secrets.

— Je fais le produits $n = pq$ et le produit $m = (p-1)(q-1)$.

— Je considère un entier e premier avec m

Les clés publiques sont n et e.

(1) Vérifier que $8^7 \equiv 2 \pmod{55}$

(2) En déduire le reste dans la division euclidienne de 8^{21} par 55.

(3) Vérifier que $8^2 \equiv 9 \pmod{55}$

(4) En déduire le reste dans la division euclidienne de 8^{23} par 55.

(5) Montrer que 23 et 40 sont premiers entre eux. En déduire, d'après l'identité de Bézout, qu'il existe des entiers relatifs u et v tels que $23u + 40v = 1$.

(6) En déduire qu'il existe un entier (positif) d, $1 < d < 40$ tel que $23d \equiv 1 \pmod{40}$.

(7) Montrer que si p et q sont des nombres premiers, alors $m = (p-1)(q-1)$ est le nombre de nombres compris entre 1 et n et premiers avec $n = pq$.

(8) On prend $p = 5$ et $q = 11$. Vérifier que ces nombres sont premiers. Calculer le nombre m de nombres premiers avec n.

(9) On choisit $e = 23$. Quelle est la clé publique ? Calculer l'entier d inverse de e pour la multiplication modulo m.

(10) Le nombre reç est 17. Quelle est la valeur du nombre émis ?