Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du 11 février 2014 : divisibilité et relation de congruence dans $\mathbb{Z}$

1 Définition et premières propriétés des congruences

Définition 1.1 *Soit n un entier naturel. Etant donnés deux entiers a et b de $\mathbb{Z}$, on dit que "a est congru à b modulo n", et l'on note "$a \equiv b \pmod{n}$" ou "$a \equiv_n b$" si $a - b \in \mathbb{Z}$.*

Exemple $2014 \equiv_2 0$; $2014 \equiv_2 4102$

Lemme 1.1 *$a \equiv_n b$ si et seulement si a et b ont le même reste dans la division euclidienne par n.*

Preuve : Soit (q_a, r_a) et (q_b, r_b) les deux couples uniques d'entiers $0 \leq q_a, q_b < n$ et $a = q_a n + r_a$ et $b = q_b n + r_b$. $a - b = (q_a - q_b)n + (r_a - r_b)$. $a - b \in n\mathbb{Z}$ si et seulement si $r_a - r_b \in n\mathbb{Z}$. Or $-n < r_a - r_b < n$ et $]-n, n[\cap n\mathbb{Z} = \{0\}$ donc $r_a = r_b$ $\square$

1.1 étude de la relation de congruence modulo n

Soit $n \in \mathbb{N}$ donné, dans $\mathbb{Z}$, la relation $\equiv_n$ satisfait les propriétés de

réflexivité : $\forall a \in \mathbb{Z}, a \equiv_n a$ car $0 \in n\mathbb{Z}$

symétrie : $\forall a, b \in \mathbb{Z}, a \equiv_n b \Leftrightarrow b \equiv_n a$ car $n\mathbb{Z}$ est stable par opposé.

transitivité : : $\forall a, b, c \in \mathbb{Z}, a \equiv_n b$ et $b \equiv_n c \Rightarrow a \equiv_n c$ car $n\mathbb{Z}$ est stable par addition.

Les relations possédant ces trois propriétés forment une classe de relation très importante, d'où la définition suivante.

Définition 1.2 (Relation d'équivalence) *Une relation $\mathcal{R}$ réflexive, symétrique et transitive sur un ensemble E non vide est appelée une (relation)* équivalence *sur E.*

L'égalité (définie comme l'identité) est la relation d'équivalence généralement disponible sur tout ensemble. Ses classes d'équivalence sont réduites aux singletons. C'est la seule relation qui est à la fois une relation d'ordre et une relation d'équivalence.

Dans l'ensemble des humains, la relation "être né la même année" est une relation d'équivalence. La relation "ressembler à" n'est pas une relation d'équivalence (cf. la sorite du chevelu du TD 1).

$\equiv_n$ dans $\mathbb{Z}$ est en fait un cas particulier de relations d'équivalences, celles définies à l'aide d'une fonction. En effet, il s'agit de la fonction de $\mathbb{Z}$ dans $\mathbb{Z}$ qui a tout entier relatif a associe son le reste par la division euclidienne par n. On a le théorème qui suit, dont la preuve est triviale.

Théorème 1.1 *Soit f une application (ou fonction totale) définie d'un ensemble E dans un ensemble F, la relation définie sur E par $x \sim_f y$ si $f(x) = f(y)$ est une relation d'équivalence.*

Définition 1.3 (Classe d'équivalence) *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E non vide. Une partie A non vide de E telle que*

$$\forall a, a' \in A, a\mathcal{R}a' \quad et \quad \forall a \in A, \forall b \notin A, a(\neg\mathcal{R})b$$

est appelée classe d'équivalence de $\mathcal{R}$.

Soit $a \in E$, l'image de a par $\mathcal{R}$, $\mathcal{R}(a) = \{b \in E, a\mathcal{R}b\}$ est appelée classe d'équivalence de a modulo $\mathcal{R}$ et est notée $[a]_\mathcal{R}$.

Les classes d'équivalence des relations de congruence modulo n sont appelées *classes de congruence modulo n.*

classes de congruence modulo 0 : $a \equiv_0 b \Leftrightarrow a = b$. Il s'agit donc de la relation d'égalité sur $\mathbb{Z}$.

classes de congruence modulo 1 : $a \equiv_1 b \Leftrightarrow a - b \in \mathbb{Z}$. Il s'agit donc de la relation d'indifférence sur $\mathbb{Z}$. Il n'y a qu'une seule classe de 1-congruence.

1.1.1 Propriétés générales des relation d'équivalence

La réflexivité d'une relation $\mathcal{R}$ sur un ensemble E permet à l'union des classes d'équivalence $\mathcal{R}$ dans E de recouvrir E car $\forall x \in E, x \in [x]_\mathcal{R}$. Si la relation $\mathcal{R}$ est une équivalence, on a de plus

Proposition 1.2 *Soit $\mathcal{R}$ une équivalence sur un ensemble E,*

$$\forall a, b \in E, a\mathcal{R}b \Leftrightarrow [a]_\mathcal{R} = [b]_\mathcal{R}.$$

Preuve. $\Rightarrow$: Supposons $a\mathcal{R}b$, montrons que $[a]_\mathcal{R} \subseteq [b]_\mathcal{R}$. Soit $c \in [a]_\mathcal{R}$, $a\mathcal{R}c$ par définition et $c\mathcal{R}a$ par symétrie. Par transitivité, on a $c\mathcal{R}b$, soit $c \in [b]_\mathcal{R}$, donc $[a]_\mathcal{R} \subseteq [b]_\mathcal{R}$.

En échangeant les rôles de a et b, on obtient $[b]_\mathcal{R} \subseteq [a]_\mathcal{R}$, d'òu l'égalité cherchée.

$\Leftarrow$: Supposons $[a]_\mathcal{R} = [b]_\mathcal{R}$, par réflexivité, $a \in [a]_\mathcal{R}$, or $b\mathcal{R}a$ donc a et b appartiennent à la même classe déquivalence, ils sont donc équivalents : $a\mathcal{R}b$ □

Corollaire 1.1 *Soit $\mathcal{R}$ une équivalence sur un ensemble E, et C une classe déquivalence, alors $\forall a \in C$, $C = [a]_\mathcal{R}$.*

Tout élément $a \in C$ est appelé un représentant de la classe C.

En effet, $C \neq \emptyset$, donc $\exists c \in C, C = [c]_\mathcal{R}$, et par définition de C, $\forall a \in C a\mathcal{R}c$, $\forall a \notin C, (\neg\mathcal{R})c$.

Proposition 1.3 (relation d'équivalence et partition) *Soit $\mathcal{R}$ une équivalence sur un ensemble E, les classes d'équivalence de $\mathcal{R}$ forment une partition de E, c'est-à-dire que E est l'union disjointe des classes d'équivalence de $\mathcal{R}$.*

Preuve : Soit C une classe déquivalence de E. C'est une partie non vide de E.

Soit C et C' deux classes d'équivalence différentes. Montrons qu'elles sont disjointes. Comme ces deux classes ne sont pas identiques, l'une d'elle, disons C, contient un élement c non contenu dans C', c'est-à dire que $\forall c' \in C'$, $c(\neg\mathcal{R})c'$. Par définition d'une relation déquivalence, $\forall c' \in C', c' \notin C$. Deux classes déquivalence différentes sont donc disjointes.

Il nous reste à prouver que l'union des classes déquivalence recouvre E.
Or $\forall a \in E, a \in [a]_\mathcal{R}$ □

Proposition 1.4 *Soit f une application d'un ensemble E non vide dans un ensemble F, Les classes d'équivalence des relations $\sim_f$ sont en correspondance bijective avec $f(E)$.*

Preuve Par définition de $\sim_f$.

Corollaire 1.2 *classes de congruence modulo n, $n > 1$: $\mathbb{Z}$ possède exactement n classes de congruence modulo n. Ces classes sont infinies, disjointes deux à deux et leur union égale $\mathbb{Z}$.*

La proposition 1.4 permet la création d'un nouvel ensemble d'importance,

Définition 1.4 (ensemble quotient) *Soit $\mathcal{R}$ une relation d'équivalence sur E, l'ensemble $\{C_i, i \in I\}$ des classes d'équivalence de $\mathcal{R}$ est appelé ensemble quotient de E par la relation $\mathcal{R}$ et est notée $E/\mathcal{R}$.*

D'après le corollaire 1.1, $\exists (a_i)_{i\in I} \subseteq E$, tel que $E/\mathcal{R} = \{[a_i]_\mathcal{R}, i \in I\}$.

On dit que $(a_i)_{i\in I}$ est un système de représentant de de $E/\mathcal{R}$, car il contient un et un seul élément de chaque classe d'équivalence.

On vient donc de définir de nouveaux objets, les classes d'équivalence, et un nouvel ensemble, l'ensemble des classes d'équivalence, ou ensemble quotient. La bijection qui existe entre l'ensemble quotient et un système de représentants, nous interpelle sur la

possibilité de définir dans $E/\mathcal{R}$ des opérations similaires aux opérations définies dans E: faire sur les classes ce qu'on peut faire sur les représentants. Il faut pour cela que le résultat des opérations ne dépendent pas du choix du système de représentants. Il faut donc commencer par vérifier le comportement des opérations vis-à-vis de la relation d'équivalence. C'est ce que l'on va commencer par faire sur les congruences modulo n.

1.2 Opérations arithmétiques et congruence modulo n

Proposition 1.5 *Soit $n \in \mathbb{N}, n > 1$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv_n b$ et $c \equiv_n d$, alors*

1. *compatibilité avec l'addition $a + c \equiv_n b + d$*
2. *compatibilité avec le passage à l'opposé $-a \equiv_n -b$*
3. *compatibilité avec la multiplication $a\,c \equiv_n b\,d$*
4. *stabilité par somme $k + a \equiv_n k + b$, $\forall k \in \mathbb{Z}$*
5. *stabilité par multiplication $ka \equiv_n kb$, $\forall k \in \mathbb{Z}$*
6. *stabilité puissance $a^k \equiv_n b^k$, $\forall k \in \mathbb{N}_*$*

Preuve :

1. compatibilité avec l'addition : $a - b \in n\mathbb{Z}$ et $c - d \in n\mathbb{Z} \Rightarrow (a + c) - (b + d) \in n\mathbb{Z}$ par propriété arithmétique de $\mathbb{Z}$ et stabilité additive de $n\mathbb{Z}$
2. compatibilité par passage à l'opposé car $n\mathbb{Z}$ est stable par passage à l'opposé. On en déduit donc la compatibilité avec la soustraction $a - c \equiv_n b - d$
3. compatibilité avec la multiplication $a - b \in n\mathbb{Z}$ et $c - d \in n\mathbb{Z}$. Or $ac - bd = ac - bc + bc - bd$. Donc $ac - bd = (a - b)c + b(c - d) \in n\mathbb{Z}$
4. trivial
5. $ka - kb = k(a - b)$
6. Par récurrence : posons P(k) = $a^k \equiv_n b^k$. P(1) est vrai par hypothèse sur a et b. Montrons que $P(k) \Rightarrow P(k + 1)$.
   $a^{k+1} = a.a^k \equiv_n$ [Hyp P(k), P(1) et compatibilité avec la multiplication] $b.b^k = b^{k+1}$.
   Comme $P(1)$, et $P(k) \Rightarrow P(k + 1)$, l'identité est démontrée pour tout $\forall k \in \mathbb{N}_*$.

Attention

$$ma \equiv_n mb \not\Rightarrow a \equiv_n b$$

$22 \equiv_{10} 32$ mais $11 \equiv_{10} 16$

Remarque : Une *congruence* est une relation d'équivalence compatible avec les opérations internes de l'ensemble. Les congruences modulo n sont donc bien des congruences de $\mathbb{Z}$.

Proposition 1.6 *Soit* $n \in \mathbb{N}, n > 1$, $a, b \in \mathbb{Z}_*$, $m \in \mathbb{Z}_*$

$$Si \quad (m \wedge n = 1), \quad alors \quad (m.a \equiv_n m.b \Rightarrow a \equiv_n b)$$

Preuve : m est régulier pour la multiplication dans $\mathbb{Z}$. .
$m.a \equiv_n m.b \Leftrightarrow \exists k \in \mathbb{Z}$, tel que $ma - mb = m(a-b) = kn$. D'après le théorème de Gauss, $m \wedge n \Leftarrow m|k$, c'est-à-dire que $\exists k' \in \mathbb{Z}*, k = mk'$. Donc $m(a-b) = mk'n$ et $a - b = k'n$.

Les identités 1 et 2 de la proposition sont fondamentales car elles permettent de définir une addition et une multiplication entre classes de même congruence. En effet, elles disent que la classe de la somme [resp. du produit] d'un élément quelconque d'une classe A avec un élément quelconque d'une classe B est indépendant du choix des éléments, c'est-à-dire que l'ensemble des classes possède ces opérations comme opérations internes. Nous verrons que les congruences sont des moyens de construire de nouvelles structures.

Exemples d'application à l'arithmétique.
• $4321 + 89639$ est multiple de 9
• $4321 \times 89639 \equiv_9 1 \times 8 = 8 \equiv_9 -1$
• $10^{100} \equiv_7 3^{2\times7\times7+2} = (3^2)^{50}$.
Or $3^2 = 9 \equiv_7 2$ d'où $10^{100} \equiv_7 2^{50} =$.
Or $2^3 \equiv_7 1$ et $50 = 3 \times 16 + 2$. Donc $10^{100} \equiv_7 2^{50} \equiv_7= 2^2 = 4$.

Exemple d'application aux calendriers.

Calcul du nom du jour de tous les premiers de mois de 2014 connaissant le nom du jour du premier de l'an. 2014 est une année ordinaire. Une semaine est composée de 7 jours, chaque nom de jour de la semaine revient tous les 8 jours, c'est-à-dire que $8 \equiv_7 1$. Le *Mercredi* est le nom du jour du premier janvier.

Table 1: nombre correspondant à chaque nom de jour pour 2014

mercredi	jeudi	vendredi	samedi	dimanche	lundi	mardi
1	2	3	4	5	6	7

Le passage du premier d'un mois au premier du mois suivant correspond à un décallage de 28, 30 ou 31 jours selon le mois : pour passer du premier janvier au premier février, il faut se décaller de 31 jours, nombre de jours du mois de janvier. Or $28 \equiv_7 0$, $30 \equiv_7 2$, $31 \equiv_7 3$. Deux jours portent le même nom si leurs quantièmes dans l'année sont congrus modulo 7. Le tableau 1 attribue

Table 2: nom du premier jours du mois pour 2014

	janvier	février	mars	avril	mai	...
nombre jours	31	28	31	30	31	
modulo quantième du	1	$1+31$	1+31+28	1+31+28+31	1+31+28+31+30	...
premier dans l'année	$\equiv_7 1$	$\equiv_7 4$	$\equiv_7 4$	$\equiv_7 7$	$\equiv_7 2$	...
nom du premier	mercredi	samedi	samedi	mardi	jeudi	...

Une année ordinaire commence et finit par le même jour de la semaine. En effet il y a 7 mois de 31 jours, 4 mois de 30 jours et 1 mois de 28 jours donc : $365 \equiv_7 4 \times 30 \equiv_7 4 \times 2 \equiv_7 1$.

2 systèmes de congruence

Théorème 2.1 (théorème des restes chinois) *Soit n_1 et n_2 deux entiers premiers entre eux, et u_1, u_2 un couple d'entiers satisfaisant $u_1 n_1 + u_2 n_2 = 1$. Alors $\forall r_1, r_2 \in \mathbb{Z}$, le système de congruence*

$$(*) \begin{cases} x \equiv r_1 \quad (n_1) \\ x \equiv r_2 \quad (n_2) \end{cases}$$

est équivalent à l'unique congruence

$$x \equiv r_2(u_1 n_1) + r_1(u_2 n_2) \quad (n_1 n_2)$$

Preuve :
Posons $r = r_2(u_1 n_1) + r_1(u_2 n_2)$; alors $r \equiv r_1[u_2 n_2] \quad (n_1)$.
Mais $u_2 n_2 + u_1 n_1 = 1$ donc $u_2 n_2 \equiv 1 \quad (n_1)$, donc $r \equiv r_1 \quad (n_1)$.
De même $r \equiv r_2 \quad (n_2)$. Donc r vérifie et le système (*) et la congruence unique.
Soit x vérifiant le système (*). alors $x - r$ est un multiple de $n_1 n_2$ donc $x - r \in n_1\mathbb{Z} \cap n_2\mathbb{Z}$, or $n_1 \wedge n_2 = 1$, donc $x - r \in n_1 n_2 \mathbb{Z}$, c'est-à-dire que x vérifie l'unique congruence.

Réciproquement, si x vérifie la congruence unique, $\exists k \in \mathbb{Z}$ tel que $x = r_2 u_1 n_1 + r_1 u_2 n_2 + k n_1 n_2$, donc $x = r_1 u_2 n_2 + (r_2 u_1 + k n_2) n_1$ Or $1 = u_1 n_1 + u_2 n_2$ donc $r = r_1(1 - u_1 n_1) + (r_2 u_1 + k n_2) n_1 \equiv r_1 \quad (n_1)$
et de même $x \equiv r_2 \quad (n_2)$ □

Exemple : Pour résoudre

$$\begin{cases} x \equiv 5 \quad (8) \\ x \equiv 9 \quad (11) \end{cases}$$

comme $8 \wedge 11 = 1$, et $3.11 - 4.8 = 1$, posons $r_1 = 5, n_1 = 8, u_1 = -4, r_2 = 9, n_2 = 11, u_2 = 3$ et $r = -123$, il suffit de résoudre

$$x \equiv -123 \equiv 53 \quad (88)$$

soit $x \in \{53 + 88k, k \in \mathbb{Z}\}$

2.0.1 généralisation

L'Exemple classique Une bande de 17 pirates s'est emparé d'un butin composé d'écus de même valeur. Ils décident de se les partager équitablement et de donner le reste, qui s'élève à 3 écus, au cuisinier chinois. Mais avant le début du partage, les pirates se chamaillent et six d'entre eux sont tués. Le partage équitable entre les pirates restant, laisse au cuisinier 4 écus. Mais survient alors un naufrage et seuls 6 pirates, le cuisinier et le trésor sont sauvés. Ce dernier partage laisse 6 écus au cuisinier. Quelle est alors la fortune minimale que peut espérer ce dernier s'il décide d'empoisonner les 6 pirates survivants ?

Mise en équation du problème Il s'agit de trouver le plus petit x strictement positif vérifiant le système

$$(*)\begin{cases}(i) & x \equiv 3 \quad (17)\\ (ii) & x \equiv 4 \quad (11)\\ (iii) & x \equiv 5 \quad (6)\end{cases}$$

Résolution du système

• On constate de $17 \wedge 11 = 1$, et $2 \times 17 - 3 \times 11 = 1$ donc nous pouvons appliquer le théorème chinois au système de congruence (i et (ii) en posant

$n_1 = 17$	$u_1 = 2$	$r_1 = 3$
$n_2 = 11$	$u_2 = -3$	$r_2 = 4$

et $r = r_2(u_1 n_1) + r_1(u_2 n_2) = 4.2.17 + 3(-3)11 = 37.$

• Le système $(*)$ est équivalent au système

$$(**)\begin{cases}(i\&ii) & x \equiv 37 \quad (187)\\ (iii) & x \equiv 5 \quad\quad (6)\end{cases}$$

D'après le théorème des restes chinois (puisque 17, 11 et 6 sont premiers entre eux deux à deux, $187 \wedge 6 = 1$), et par division euclidienne $187 = 6.31 + 1$ donc en posant

$n_1 = 187$	$u_1 = 1$	$r_1 = 37$
$n_2 = 6$	$u_1 = -31$	$r_2 = 5$

et $r = r_2(u_1 n_1) + r_1(u_2 n_2) = -5947.$

La solution cherchée satisfait donc

$$x \equiv -5947 \quad (1122).$$

Résolution du problème

$x = -5947 + k.1122$, avec $k \in \mathbb{Z}$ donnant la plus petite valeur positive pour x, soit le reste de la division euclidienne de -5947 par 1122 qui est[1] 785.

[1] Attention : $-(947 = 6.(-1122) + 785$

Interprétation du résultat dans les termes du problème posé Si le cuisinier chinois empoisonne les 6 pirates restant, il garde le trésor entier, constitué d'au minimum 785 écus.

Théorème 2.2 (théorème chinois généralisé) *Soit $k \in \mathbb{N}, k \geq 2$, $n_{1,2},\cdots,_k$ k entiers naturels premiers entre eux deux à deux, et k $r_1, r_2, ..., r_k \in \mathbb{Z}$. Le système de congruences*

$$(*)\begin{cases} x \equiv r_1 \quad (n_1) \\ x \equiv r_2 \quad (n_2) \\ \cdots \\ x \equiv r_k \quad (n_k) \end{cases}$$

est équivalent à l'unique congruence

$$x \equiv \sum_{i=1}^{k} r_i U_i N_i \quad (\prod_{i=1}^{k} n_i)$$

avec $N_i = \dfrac{\prod_{j=1}^{k} n_j}{n_i}$ *et* U_i *tel que* $U_i N_i + u_i n_i = 1$

Le principe de la preuve est identique au théorème chinois :

Posons $N_i \wedge n_i = 1$d'où l'existence de u_i et v_i d'après l'identité de Bezout satisfaisant $N_i U - i + n_i u_i = 1$. posons $R = U_1 N_1 r_1 + U_2 N_2 r_2 + ... + U_k N_k r_k$, $R \equiv ri \quad (mi)$,$\forall i \in [[1, k]]$, c'est-à-dire que R est une solution du système $(*)$.

Soit a est une autre solution de $(*)$, alors $a - R \in n_i\mathbb{Z}$, $\forall i \in [[1, k]]$, donc, puisqu'ils sont premiers entre eux, $a - R \in (\prod_{i=1}^{k} n_i)\mathbb{Z}$. Autrement dit, les solutions de $(*)$ sont de la forme $x \equiv R \quad (\prod_{i=1}^{k} n_i)$. □

Attention : par rapport au théorème précédent, $u_1 = U_2$, $u_2 = U_1$, $N_1 = n_2$ et $N_2 = n_1$.

Application au problème du cuisinier chinois

• 17, 11 et 6 sont premiers entre eux deux à deux. Posons

$n_1 = 17$	$N_1 = 66$	$U_1 = 8$	$r_1 = 3$
$n_2 = 11$	$N_2 = 102$	$U_2 = 4$	$r_2 = 4$
$n_3 = 6$	$N_1 = 187$	$U_3 = 1$	$r_1 = 5$

et $R = r_1 U_1 N_1 + r_2 U_2 N_2 + r_3 U_3 N_3 = 4141$.

La solution cherchée satisfait donc

$$x \equiv 4141 \equiv 785 \quad (1122).$$