103	**Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.**	Système RSA (Terracher)	Monier De Biasi Sorosina Terracher

Prérequis: Relation d'équivalence, ensemble quotient, structure de groupe, d'anneau, de corps.

I. Congruences.

Def.1: Soient $n\in\mathbb{N}^*$, $(a,b)\in\mathbb{Z}^2$; on dit que **a est congru à b modulo n** et on note $a\equiv b\,[n]$ ssi n divise (b-a).

Exemples: $22\equiv 14\,[4]$; $13\not\equiv 8\,[4]$.

Prop.1: Pour tout $n\in\mathbb{N}^*$, la relation $\equiv\,[n]$ est une **relation d'équivalence** dans $\mathbb{Z}$. (1)

Notat°: $\forall\, n\in\mathbb{N}^*$, on notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\mathbb{Z}/\equiv\,[n]$, et $\hat{x}$ la classe d'équivalence de x dans $\mathbb{Z}/n\mathbb{Z}$. Conséquences: $\hat{x}=\{x+\lambda n / \lambda\in\mathbb{Z}\}$. Grâce à la division Euclidienne par n, on voit que $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments, et que $\mathbb{Z}/n\mathbb{Z}=\{\hat{0},\hat{1},\ldots,\widehat{n-1}\}$.

Prop.2: Soit $n\in\mathbb{N}^*$. On a, pour tout $(a,b,c,d)\in\mathbb{Z}^4$:
$$\begin{cases} a\equiv b\,[n] \\ c\equiv d\,[n] \end{cases}\Rightarrow\begin{cases} a+c\equiv b+d\,[n] \\ ac\equiv bd\,[n] \end{cases}$$ (2)
La relation d'équivalence $\equiv\,[n]$ est **compatible** avec les lois + et × de $\mathbb{Z}$.

Corollaire: $\forall(a,b)\in\mathbb{Z}^2$, $\forall k\in\mathbb{N}^*$, $\left(a\equiv b\,[n]\Rightarrow a^k\equiv b^k\,[n]\right)$.

Application 1 (BIA): **Ecriture d'un nombre en base b.** (3)
Etant donné un entier naturel $b\geq 2$, pout tout $a\in\mathbb{N}$, il existe une suite finie unique $x_0,x_1,\ldots,x_n$ avec $x_n\neq 0$ et $\forall i\in[\![0,n]\!], x_i\in[\![0,b-1]\!] / a=x_nb^n+x_{n-1}b^{n-1}+\ldots+x_1b+x_0$
C'est l'écriture du nombre a dans la base b.

Application 2 (BIA): **Critères de divisibilité.** (4)
- Un entier naturel est divisible par 2 (resp. par 5) ssi son chiffre des unités est divisible par 2 (resp. par 5).
- Un entier naturel est divisible par 3 (resp. par 9) ssi la somme de ses chiffres est divisible par 3 (resp. par 9).
- Un entier naturel est divisible par 11 ssi la différence entre la somme de ses chiffres d'indices pairs et la somme de ses chiffres d'indices impairs est divisible par 11.

Application 3 (BIA): **Preuve par 9.** (5)
Dans un produit p=ab, si l'opération est juste, alors:
soit r le reste de la division par 9 du produit p,
soit r' le reste de la division par 9 du facteur a,
soit r'' le reste de la division par 9 du facteur b,
on doit avoir r = r'.r''
(cela n'implique pas que l'opération est juste).

II. Anneau $\mathbb{Z}/n\mathbb{Z}$.

D'après ce qui précède, on peut définir, pour tous $\hat{x},\hat{y}\in\mathbb{Z}/n\mathbb{Z}$, les éléments $\widehat{x+y}\in\mathbb{Z}/n\mathbb{Z}$ et $\widehat{x.y}\in\mathbb{Z}/n\mathbb{Z}$ et ces classes seront indépendantes des représentants choisis, ce qui définit des LCI $\hat{+}$ et $\hat{.}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Prop.3: $(\mathbb{Z}/n\mathbb{Z},+,.)$ est un **anneau commutatif.** (6)

Th.1 (SOR): **Théorème Chinois.** (7)
Si $a\wedge b=1$, alors $\mathbb{Z}/ab\mathbb{Z}\simeq\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$.
Ce théorème s'étend par récurrence au cas de p nombres premiers entre eux deux à deux.

Application4 (SOR): **Congruences simultanées** (8)
Soient $\alpha,\beta\in\mathbb{Z}$. Soient $a,b\in\mathbb{N}^*$ premiers entre eux.
Le système $(S)\begin{cases} x\equiv\alpha\,[a] \\ x\equiv\beta\,[b] \end{cases}$ admet des solutions ds $\mathbb{Z}$.
La recherche de la durée séparant les passages par deux positions successives identiques de deux astres dont les périodes de révolution sont connues conduit à ce type de système (connu des Chinois, d'où le th. préc).
Exercice: Résoudre $(S)\begin{cases} x\equiv 7\,[8] \\ x\equiv 1\,[13] \end{cases}$ d'inconnue $x\in\mathbb{Z}$. (302)

Prop.4: Pour $n\in\mathbb{N}^*$, les **éléments inversibles** de $\mathbb{Z}/n\mathbb{Z}$ sont les $\hat{x}$, où $x\in\mathbb{Z}$ et $x\wedge n=1$. (9)
Exemple: les élts inversibles de $\mathbb{Z}/9\mathbb{Z}$ sont $\hat{1},\hat{2},\hat{4},\hat{5},\hat{7},\hat{8}$.

Application 5 (SOR): **Indicateur d'Euler** (10)
L'indicateur d'Euler $\varphi(n)$ de $n\in\mathbb{N}^*$ est le nombre d'entiers compris entre 1 et n, premiers avec n, c'est-à-dire le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
Si $a\wedge b=1$, alors $\varphi(ab)=\varphi(a)\varphi(b)$, formule qui s'étend à k nombres premiers entre eux deux à deux.
Pour p premier, $\varphi(p^r)=p^r\left(1-\frac{1}{p}\right)$.
Si la décomposition en facteurs premiers de n est $n=\prod_{i=1}^{N}p_i^{r_i}$, alors il vient $\varphi(n)=n\prod_{i=1}^{N}\left(1-\frac{1}{p_i}\right)$.

(BIA) **Th. d'Euler**: Si $a\wedge n=1$, $a^{\varphi(n)}\equiv 1\,[n]$.

(BIA) **Pt. Th. de Fermat**: si n premier et $n\nmid a$, $a^{n-1}\equiv 1\,[n]$.

Prop.5(Meu): Soit $p\in\mathbb{N}^*$. Les trois propriétés suivantes sont équivalentes:
(i) p est **premier**
(ii) $\mathbb{Z}/p\mathbb{Z}$ est un **corps** (commutatif)
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre (104-De Biasi)(11)

III. Applications à la cryptographie.

Application 6(TER): **Chiffrement affine**. (302-304-159)
On assimile les lettres de l'alphabet A, B, ...Z aux nombres 0,1,...,25, et on code ces nombres par la fonction de "hachage": $f:\begin{cases}\{0,1,...,25\}\to\{0,1,...,25\}\\ x\mapsto f(x)\equiv 17x+22\,[26]\end{cases}$.
f(x) est le reste de la division Eucle de (17x+22) par 26
Jules César utilisait un chiffrement affine f(x)=1x+3.

Application 7(TER): **Système R.S.A.** (302)
Soient $p\neq 2$ et $q\neq 2$ deux nombres premiers distincts. On pose n=pq et soit:
e $\in\mathbb{N}$ tq. $e\in[\![1;(p-1)(q-1)[\![$ et $e\wedge[(p-1)(q-1)]=1$.
Alors $\exists!\, d\in[\![1;(p-1)(q-1)[\![$ et $ed\equiv 1[(p-1)(q-1)]$ et $\forall m\in\mathbb{N}, m^{ed}\equiv m[n]$.
Utilisation pour que A transmette des informations à B:
1) B choisit p et q premiers distincts, et $e\in[\![1;(p-1)(q-1)[\![$ tq $e\wedge[(p-1)(q-1)]=1$.
2) B calcule d
3) B diffuse n=pq et d.
4) Pour envoyer un message à B, A convertit ce message en une suite de nombres m ≤ n. Pour chiffrer chacun de ces nombres m, A calcule $c\in[\![1,n]\!]$ tq $m^e\equiv c[m]$. A envoie c à B.
5) B déchiffre c, en calculant $c^d[n]$.

IV. Notes.

(BIA)De Biasi. (TER) Terracher T.S. (SOR) Sorosina algèbre.
°Modifs /ordre du bouquin.
N.B.: Arithmétique modulaire (utilisant la congruence).
(1) Réflexive, Symétrique, Transitive.

(2) Ecrire $a\equiv b[n]$ comme $(b-a)=\lambda n$, et faire une vérif. directe en s'assurant que la coef obtenu est ds $\mathbb{Z}$.

(3) (BIA)**Ecriture d'un nombre en base b**.
$\exists!x_0\in\mathbb{N}$: $a=bq_0+x_0$, avec $0\leq x_0<b$ et $q_0<a$.
On divise ainsi le quotient obtenu autant de fois que possible: $\exists!x_1\in\mathbb{N}$: $q_0=bq_1+x_1$, avec $0\leq x_1<b$ et $q_1<a$.
puis $\exists!x_2\in\mathbb{N}$: $q_1=bq_2+x_2$, avec $0\leq x_2<b$ et $q_2<a$...
On obtient $a=b^n n_n+...+b^2x_2+bx_1+x_0$.

(4) (BIA)**Critère de divisibilité**. Soit a l'entier d'écriture décimale $a=10^n x_n+10^{n-1}x_{n-1}+...+10x_1+x_0$.
Div. par 2 et 5: 2 et 5 sont des diviseurs de 10 et dons de 10^k pour tout $k\in\mathbb{N}^*$. Alors $\forall k\in\mathbb{N}^*$, $10^k\equiv 0[2]\,et\,[5]$, donc $a\equiv x_0[2]\,et\,[5]$.
Div. par 3 et 9: 3 et 9 divisent 10-1, d'où $10\equiv 1[3]\,et\,[9]$.
Par suite, $\forall k\in\mathbb{N}^*, 10^k\equiv 1[3]\,et\,[9]$,
donc $a\equiv x_n+x_{n-1}+...+x_0\,[3]\,ou\,[9]$.
Div. par 11: $10\equiv -1[11]$, d'où $\forall k\in\mathbb{N}^*, 10^k\equiv(-1)^k[11]$
donc $a\equiv(-1)^n x_n+(-1)^{n-1}x_{n-1}+...+x_0\,[11]$.

(5) (BIA)**Preuve par 9**.
ab=p, a=9q+r, b=9q'+r' ⟹ ab=p=(9q+r)(9q'+r')= 81qq'+9qr'+9rq'+rr', i.e. $p\equiv rr'[9]$, i.e. les reste des divisions par 9 du produit p=ab et de rr' doivent être =.

(6) Vérif. groupe abélien pour +.
Vérif. loi "." Assoc., Commut., Neutre, et Distributive / +.

(7) (SOR)**Théorème Chinois**.
Pour $n\in\mathbb{N}^*$; on note $cl_n(x)$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$.
$\begin{matrix}\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\\ x\mapsto cl_n(x)\end{matrix}$ est surjective (surj° can.) car les $cl_n(x)$ forment une partition de $\mathbb{Z}$.
Soit $f:\begin{matrix}\mathbb{Z}/ab\mathbb{Z}\to\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}\\ \xi=cl_{ab}(x)\mapsto(cl_a(x);cl_b(x))\end{matrix}$.
→ f est bien définie: sa définition ne dépend pas du choix du représentant x de la classe ξ.
Soit $y\in\xi=cl_{ab}(x)=\{z\in\mathbb{Z}/x-z\in ab\mathbb{Z}\}$, alors ab|x-y, donc : a|x-y et b|x-y, Or:
$cl_a(x)=\{z\in\mathbb{Z}/x-z\in a\mathbb{Z}\}$ donc
$y\in cl_a(x)$, i.e. $cl_a(x)=cl_a(y)$
$cl_b(x)=\{z\in\mathbb{Z}/x-z\in b\mathbb{Z}\}$ donc $cl_b(x)=cl_b(y)$
Ainsi, si x et y sont deux représentants de ξ, alors f(x)=f(y), et f est bien définie.
→ f est un morphisme d'anneaux:
Compatibilité avec +: vient de cl(x+y) = cl(x) + cl(y), Prop. 2. De même pour la compatibilité avec ×.
Transport de l'unité: $f(cl_{ab}(1))=(cl_a(1);cl_b(1))$.
→ f est bijective: Comme f est définie entre deux anneaux finis de même cardinal, il suffit de prouver l'injectivité, i.e. Ker(f)={$cl_{ab}(0)$}.
soit $x\in\mathbb{Z}$ tq $f(cl_{ab}(x))=(cl_a(0);cl_b(0))$.
Alors $cl_a(x)=cl_a(0)$, donc a|x. De même, b|x. Comme $a\wedge b=1$, ab|x, donc $cl_{ab}(x)=cl_{ab}(0)$, ce qui montre l'injectivité et par suite la bijectivité.
Finalement, f est bien un isomorphisme.
(+4) *N.B.: l'hypothèse $a\wedge b=1$ est bien nécessaire, contre-exemple*** $\mathbb{Z}/8\mathbb{Z}\not\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.
(Wikipedia) Forme originale (congruences simultanées) Qin Jiushao publié en 1247. Mais on trouve trace d'un pb analogue dans le livre de Sun Zi, le Sunzi suanjing datant du IIIe siècle :

*→Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il **reste** deux soldats, rangés par 5 colonnes, il **reste** trois soldats et, rangés par 7 colonnes, il **reste** deux soldats ? >Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.*
→Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ? >Si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, la question se traduit par : Existe-t-il un entier x tel que le reste de la division de x par 365 donne 6 et le reste de la division de x par 28 donne 3 ?
→Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

(8) (SOR)**Congruences simultanées** (forme originale du th. Chinois).

$(S) \Leftrightarrow (cl_a(x); cl_b(x)) = (cl_a(\alpha); cl_b(\beta)) \Leftrightarrow$

$f(x) = (cl_a(\alpha); cl_b(\beta))$ et f surjective assure $\exists x$.

(9) **a)** Soient $\xi \in \mathbb{Z}/n\mathbb{Z}$ inversible et $\zeta \in \mathbb{Z}/n\mathbb{Z}$ son inverse. On a $\xi\zeta = \hat{1}$ et avec des représentants respectifs des classes: $\hat{x}\hat{y} = 1$, donc $xy - 1 = kn$, i.e. $xy - kn = 1$, i.e. (Bézout) $x \wedge n = 1$.

b) Réciproquement, soit x tq $x \wedge n = 1$, il existe (Bézout) u,v dans $\mathbb{Z}$ tq $xu + nv = 1$, alors (en notant toujours ξ la classe de x):

$\hat{1} = \widehat{xu + nv} = \hat{x}\hat{u} + \hat{n}\hat{v} = \hat{x}\hat{u} + \hat{n}\hat{v} = \xi\hat{u} + \hat{0} = \xi\hat{u}$, ce qui montre que ξ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

(10) (SOR)**Indicateur d'Euler**.
Avec les notations du (4), $f : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est un isomorphisme d'anneaux, donc transporte les éléments inversibles (notés ici (...)*).
Alors $(\mathbb{Z}/ab\mathbb{Z})^* \simeq (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ **(1)**
On dira que $f : \mathbb{N}^* \to \mathbb{Z}$ est **arithmétique multiplicative** ssi $\forall (a,b) \in (\mathbb{N}^*)^2, (a \wedge b = 1 \Rightarrow f(ab) = f(a)f(b))$.
Or $\forall n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z})^* = \{cl_n(x) / x \in \mathbb{Z}, x \wedge n = 1\}$ (Pr.4)
Donc $\forall n \in \mathbb{N}^*$, $\varphi(n) = Card(\mathbb{Z}/n\mathbb{Z})^*$.
D'après **(1)**, il vient: $\varphi(ab) = \varphi(a).\varphi(b)$, et **φ arith.mult**.
Par définition de φ:

$\varphi(p^r) = Card\{k \in [\![1, p^r]\!] / k \wedge p^r = 1\}$

$= Card\{k \in [\![1, p^r]\!]\} - Card\{k \in [\![1, p^r]\!] / k \wedge p^r \neq 1\}$

On a $Card\{k \in [\![1, p^r]\!]\} = p^r$.

Or pour tout $k \in [\![1, p^r]\!]$,

$k \wedge p^r \neq 1 \Leftrightarrow p \mid k \Leftrightarrow k \in \{qp / 1 \leq q \leq p^{r-1}\}$,

où $Card\{qp / 1 \leq q \leq p^{r-1}\} = p^{r-1}$.

Donc $\varphi(p^r) = p^r - p^{r-1}$.

Comme φ est arithmétique multiplicative, pour $n = \prod_{i=1}^{N} p_i^{r_i}$, il vient $\varphi(n) = n\prod_{i=1}^{N}\left(1 - \frac{1}{p_i}\right)$

Et par suite φ est bien déterminée.

(BIA)**Th. d'Euler**: Si $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1[n]$.

Card(ℤ/nℤ)*=φ(n). Th. Lagrange: l'ordre d'un sg divise l'ordre du groupe (fini). Donc si a∈(ℤ/nℤ)*, i.e. $a \wedge n = 1$, Card<a>| Card(ℤ/nℤ)*, i.e. l'ordre de a divise φ(n), et par définition de l'ordre d'un élément, $a^{\varphi(n)}=1$ ds ℤ/nℤ, i.e. $a^{\varphi(n)} \equiv 1[n]$.

(BIA)**Pt. Th. de Fermat**: si n premier et $n \nmid a$, $a^{n-1} \equiv 1[n]$.

En particulier si n est premier, on a $\varphi(n) = n - 1$, d'où △

(11) (Meu)On démontre (i)⟹(ii)⟹(iii).
(i)⟹(ii): Supposons p premier. Tout élément de ℤ/pℤ différent de $\hat{0}$ est non divisible par p, et comme p est premier, il est premier avec p, donc inversible d'après ce qui précède. Donc ℤ/pℤ est un corps.
(ii)⟹(iii)**Tout corps commutatif est un anneau intègre**.
Si K est un corps et a,b∈K tq ab=0 et a≠0, alors $b = a^{-1}(ab) = a^{-1}.0 = 0$.
(iii)⟹(i): **Mq ¬ (i)⟹ ¬ (iii).**
Soit n composé, n=ab, avec 1<a<n et 1<b<n. Alors $\hat{a}\hat{b} = \widehat{ab} = \hat{n} = 0$, avec $\hat{a} \neq \hat{0}$ et $\hat{b} \neq \hat{0}$, donc ℤ/nℤ n'est pas intègre (on a exhibé des diviseurs de zéro).
On dispose ainsi d'une infinité de corps finis deux à deux non isomorphes. Il en existe d'autres.